# Gjelder det en risikobasert tilnærming til reglene i GDPR ved overføring av personopplysninger til tredjestater?

*Om innholdet i kravet til supplerende beskyttelsestiltak i lys av Schrems II-dommen*

Kandidatnummer: 1 & 139

Antall ord: 23 355


JUS399 Masteroppgave
Det juridiske fakultet

UNIVERSITETET I BERGEN

7. juni 2021

# Innholdsfortegnelse

# 1 Innledning

## 1.1 Tema og problemstilling

Oppgavens tema er overføring av personopplysninger til stater utenfor EU- og EØS-området (heretter «tredjestater»). Nærmere bestemt skal det gjøres rede for kravet om supplerende beskyttelsestiltak ved slike overføringer, som ble introdusert av EU-domstolen i sak C-311/18 (Schrems II).[1] Saken gjaldt en klage fra jurist og personvernaktivist Maximilian Schrems til det irske datatilsynet, der han krevde overføringer av hans personopplysninger fra Facebook Irland til Facebook Inc i USA stanset.[2] EU-domstolen vurderte i denne sammenheng reglene i General Data Protection Regulation[3] (heretter «GDPR», «personvernforordningen» eller «forordningen») kapittel V, som regulerer overføring[4] av personopplysninger til tredjestater. Overføringer ut av EU/EØS er i utgangspunktet ikke tillatt, med mindre man har et overføringsgrunnlag. Kapittel V gir derfor anvisning på en rekke alternative overføringsgrunnlag som kan tas i bruk for at slike overføringer kan finne sted, herunder standard personvernbestemmelser vedtatt av Kommisjonen (heretter «EUs standardkontrakter» eller «de standardiserte personvernbestemmelsene»), jf. GDPR artikkel 46 nr. 2 bokstav c.

De standardiserte personvernbestemmelsene inngås mellom eksportøren og importøren av personopplysningene, og gir partene forpliktelser som skal sikre at de overførte personopplysningene behandles i samsvar med reglene som gjelder innenfor EU/EØS.[5] Deres kontraktsrettslige natur innebærer imidlertid at de ikke er bindende for myndighetene i den tredjestaten som overføringen skjer til. Et særskilt spørsmål i Schrems II-saken var om EUs standardkontrakter av den grunn ikke lenger kan opprettholdes som et gyldig overføringsgrunnlag.[6]

[1] C-311/18 *Schrems II.*
[2] C-311/18 *Schrems II* avsnitt 77.
[3] Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF [GDPR].
[4] Ordet *overføring* er ikke definert i GDPR. I et prosjektnotat fra EDPS er derimot overføringer omtalt som der personopplysninger er «move[d] or allowed to move between different users», se EDPS Position Paper (2014) s. 6.
[5] Datatilsynet (2020).
[6] C-311/18 *Schrems II* avsnitt 127.

EU-domstolen besvarte dette spørsmålet benektende.[7] Imidlertid er det etter forholdene – der lovgivningen i tredjestaten gir dataimportøren plikter som strider mot innholdet i de standardiserte personvernbestemmelsene – påkrevd med supplerende beskyttelsestiltak som kompenserer for den lavere graden av beskyttelse som den nasjonale lovgivningen medfører.[8] Dette poenget gjør seg gjeldende på generelt grunnlag, med den konsekvens at kravet om supplerende beskyttelsestiltak også gjelder ved overføring av personopplysninger til andre tredjestater enn USA.

Hva som nærmere bestemt skal til for at de supplerende beskyttelsestiltakene skal anses for å gi tilstrekkelig beskyttelse, sa EU-domstolen imidlertid ingenting eksplisitt om. I kjølvannet av Schrems II-dommen har derimot European Data Protection Board (heretter «EDPB» eller «Personvernrådet») publisert en veileder tilknyttet dette kravet.[9] Veilederen har vært ute på høring, og er i skrivende stund ikke vedtatt i sin endelige form. Et spørsmål som i høringsrunden har vært gjenstand for debatt, er Personvernrådets uttalelse om at *sannsynligheten* for at tredjestatens myndigheter ønsker tilgang til de overførte personopplysningene ikke er en relevant faktor for vurderingen av beskyttelsesnivået ved den konkrete overføringen.[10] Flere aktører har i høringsrunden vist til hvordan GDPR gjennomsyres av en risikobasert tilnærming, og at denne tilnærmingen også må gjelde ved overføringer.[11] Andre aktører, deriblant den ideelle organisasjonen None Of Your Business (NOYB), forfekter Personvernrådets holdning til sannsynlighetsvurderinger, og viser til at de risikobaserte bestemmelsene i GDPR ikke gjelder forordningens kapittel V om overføring til tredjestater.[12]

Oppgavens nærmere problemstilling er hvorvidt det må tas utgangspunkt i en risikobasert tilnærming ved vurderingen av hvilke beskyttelsestiltak som er tilstrekkelige. I forlengelsen av dette vil det også vurderes hva som er de praktiske konsekvensene av en slik tilnærming.

---

[7] C-311/18 *Schrems II* avsnitt 149.
[8] C-311/18 *Schrems II* avsnitt 132.
[9] EDPB Recommendations 01/2020.
[10] EDPB Recommendations 01/2020 s. 14, avsnitt 42.
[11] Se eksempelvis DLA Pipers høringsuttalelse: https://blogs.dlapiper.com/privacymatters/dla-piper-comments-on-edpb-recommendations-01-2020-on-measures-that-supplement-transfer-tools-to-ensure-compliance-with-the-eu-level-of-protection-of-personal-data/ (sist lest 04.02.2021).
[12] Link til NOYBs høringsuttalelse: https://noyb.eu/sites/default/files/2020-12/Feedback_SCCs_nonEU.pdf (sist lest 08.02.2021).

## 1.2 Bakgrunn og aktualitet

Utfordringene knyttet til overføring av personopplysninger til tredjestater har blitt en særlig aktuell bekymring etter de såkalte Snowden-avsløringene i 2013. IT-tekniker og tidligere CIA-ansatt Edward Snowden lekket dette året gradert informasjon om hvordan amerikanske myndigheter overvåket nasjonale og utenlandske borgere gjennom etterretningsprogrammet PRISM.[13] Avsløringene foranlediget EU-domstolens avgjørelse i Schrems I-saken[14], der domstolen la til grunn at overføring av personopplysninger til USA på grunnlag av den såkalte Safe Harbour-ordningen[15] var ulovlig. Safe Harbour var en avtale mellom EU-kommisjonen og det amerikanske handelsdepartementet, og innebar at amerikanske virksomheter kunne forplikte seg til en rekke regler som skulle bringe beskyttelsesnivået ved deres databehandling til et forsvarlig nivå.[16] For sin konklusjon viste imidlertid EU-domstolen blant annet til amerikanske myndigheters vidtgående og uproporsjonale adgang til å samle inn data,[17] og hvordan denne adgangen gikk foran virksomhetenes forpliktelser etter Safe Harbour-ordningen ved eventuell kollisjon.[18]

Saken fikk så sin oppfølger i den nevnte Schrems II-dommen[19], som ble avsagt 16. juli 2020. I tillegg til drøftelsene rundt EUs standardkontrakter, tok domstolen her stilling til gyldigheten av Privacy Shield-ordningen, som overtok for Safe Harbour som alternativ for overføring av personopplysninger til USA.[20] I denne sammenheng foretok EU-domstolen en grundigere gjennomgang av amerikanske overvåkningshjemler, nærmere bestemt «Foreign Intelligence Act 702»[21] (FISA 702) og «Executive Order 12333»[22] (EO 12333). Her viste domstolen til at de to hjemlene ikke tok hensyn til proporsjonalitet og hva som er nødvendig i et demokratisk samfunn, og dermed ikke overholdt kravene etter EUs pakt om grunnleggende rettigheter[23] (heretter «pakten» eller «grunnrettighetspakten») artikkel 52.[24] I tillegg ble det presisert at bruken av FISA 702 og EO 12333 ikke gir de registrerte noen rett til å overprøve

[13] Restad, Notaker og Mæhlum (2019).
[14] C-362/14 *Schrems I.*
[15] Decision 2000/520/EC vedlegg I.
[16] Decision 2000/520/EC.
[17] C-362/14 *Schrems I* avsnitt 90.
[18] C-362/14 *Schrems I* avsnitt 85-86.
[19] C-311/18 *Schrems II.*
[20] Decision 2016/1250/EU.
[21] Foreign Intelligence Surveillance Act: Section 702, 50 U.S.C. § 1881 a.
[22] Excecutive Order No. 12,333, 46 Federal Regulation 59,941-42 (4. desember 1981).
[23] Charter of Fundamental Rights of the European Union (2012/C 326/02).
[24] C-311/18 *Schrems II,* avsnitt 185.

sine rettigheter i det amerikanske rettssystemet.[25] I så måte innebar overføringer til USA på grunnlag av Privacy Shield også brudd på retten til «håndhevbare rettigheter og effektive rettsmidler» etter pakten artikkel 47, med den konsekvens at heller ikke denne sertifiseringsordningen ga tilstrekkelig beskyttelse. Domstolen konkluderte derfor med at Privacy Shield er ugyldig.

Parallelt med at bevisstheten rundt myndigheters overvåkningspraksis har blitt større, har individenes personopplysninger blitt en viktig handelsvare.[26] Europakommisjonen har i rapporten «The European Data Market Monitoring Tool» fra 2020 anslått at den datadrevne økonomien kan utgjøre om lag 827 milliarder euro innen 2025,[27] og Solberg-regjeringen fremhevet i mars i år datadrevet økonomi som en viktig faktor for videre økonomisk vekst i Norge.[28] Bruken av skytjenester, som muliggjør dataprosessering og -lagring på servere på den andre siden av kloden,[29] øker stadig i omfang.[30] Sammen med denne utviklingen kommer også økte muligheter for offentlige og private aktører til å gjøre inngrep i enkeltindividers grunnleggende rett til personvern.

Personvernet anerkjennes i de fleste internasjonale instrumenter om menneskerettigheter,[31] deriblant i artikkel 8 i grunnrettighetspakten og artikkel 8 i Den europeiske menneskerettskonvensjon[32] (heretter «EMK»), og innebærer blant annet at den enkelte skal ha kontroll over og kunne bestemme over opplysninger om seg selv.[33] Balansegangen mellom behovet for fri flyt av personopplysninger og personvernet er søkt ivaretatt med nettopp GDPR, som ifølge formålsbestemmelsen i artikkel 1 skal ivareta begge disse hensynene innad i EU/EØS. Særskilte utfordringer oppstår imidlertid der personopplysningene overføres til land med andre personvernregler. Rettighetene og pliktene som følger av GDPR får naturligvis begrenset effekt dersom virksomhetene står fritt til å overføre personopplysningene til en annen jurisdiksjon, og dermed blir underlagt mildere regler.

[25] C-311/18 *Schrems II,* avsnitt 192.
[26] Wessel-Aas og Ødegaard (2018) s. 2.
[27] European Commission (2020).
[28] Meld. St. 22 (2020-2021) s. 5.
[29] Datatilsynet (2018).
[30] Nasjonal Sikkerhetsmyndighet (2020) s. 32.
[31] Wessel-Aas og Ødegaard (2018) s. 17.
[32] Den europeiske menneskerettighetskonvensjon (EMK).
[33] Regjeringen (2019).

Ettersom de fleste skytjenesteleverandører er basert utenfor Europa, er denne utfordringen svært aktuell.[34]

I tillegg til at de nevnte utfordringene med overføring av personopplysninger er aktuelle på generell basis, er det som følge av Schrems II-dommen og den etterfølgende veilederen fra Personvernrådet for øyeblikket stor usikkerhet knyttet til adgangen for europeiske aktører til å engasjere databehandlere fra stater utenfor EU/EØS. Oppgaven søker å avklare enkelte av disse uklarhetene.

## 1.3 Rettskilder, metode og utfordringer

Oppgavens problemstilling vil drøftes med grunnlag i EU-retten, med primært fokus på GDPR. Forordningen er inntatt i EØS-avtalen og «gjelder som lov» etter personopplysningsloven § 1.[35] Den norske oversettelsen av personvernforordningen vil benyttes i oppgaven.

Fortolkningen av EU-retten må ta utgangspunkt i EU-rettslig metode, slik denne er etablert og utviklet gjennom EU-domstolens praksis. Det innebærer at rettskildene skal tolkes med utgangspunkt i en naturlig språklig forståelse av ordlyden, sammenholdt med dens kontekst og formål.[36]

Medlemsstatene har forpliktet seg til EUs rettsakter gjennom artikkel 288 i Traktaten om Den europeiske unions virkemåte[37] (heretter «TEUV»), og har med dette tillagt EUs lovgivende organer autoritet. I tillegg til ivaretakelsen av forutberegnelighetshensyn, forutsetter respekten for denne maktfordelingen at rettsaktenes ordlyd forstås med utgangspunkt i normal språkbruk.[38]

Når det etter EU-rettslig metode skal foretas en formålsorientert fortolkning av rettsaktenes formuleringer, siktes det til både enkeltbestemmelsenes særskilte formål og formålet med rettsakten i sin helhet.[39] For eksempel må GDPR tolkes slik at det generelle formålet om personopplysningsvern, sammenholdt med fri utveksling av personopplysninger etter artikkel

[34] Foss (2021).
[35] Lov av 15. juni 2018 nr. 38 om behandling av personopplysninger.
[36] Se eksempelvis C-480/10 *Kommisjonen mot Sverige*, avsnitt 33.
[37] Traktaten om Den europeiske unions virkeområde (TEUV).
[38] Fredriksen og Mathisen (2014) s. 21.
[39] Fredriksen og Mathisen (2014) s. 231.

1, ivaretas. Ved overføring av personopplysninger til tredjestater må også det særskilte målet i artikkel 44 om å ikke undergrave forordningens beskyttelsesnivå ved slike overføringer hensyntas.

Hva gjelder rettsaktens kontekst er det viktig å være seg bevisst EU-rettens hierarkiske system. Rettsaktene har sitt grunnlag i traktatene inngått mellom medlemsstatene.[40] Særlig sentralt står som nevnt TEUV, samt Traktaten om Den europeiske union[41] (heretter «TEU») og pakten. Pakten har i henhold til TEU artikkel 6 «same legal value» som traktatene. I EU-retten kan det dermed skilles mellom *primærretten* – som er traktatene og pakten – og *sekundærretten* – som er de rettsaktene som fremgår av TEUV artikkel 288. Når forordninger, direktiver og annen sekundærrett skal tolkes kontekstuelt, innebærer det blant annet at de må tolkes i overenstemmelse med sitt hjemmelsgrunnlag. I motsatt fall vil de kunne bli satt til side som ugyldige.[42] For GDPRs del er det særlig artikkel 8 nr. 1 i pakten og artikkel 16 nr. 1 i TEUV – som begge gir anvisning på retten til vern av egne personopplysninger – som peker seg ut som sentrale hjemmelsgrunnlag.

EUs pakt om grunnleggende rettigheter har for øvrig fått en stadig mer fremtredende rolle i EU-domstolens praksis tilknyttet EU-rettslig sekundærrett.[43] I relasjon til GDPR innebærer dette blant annet at personvernet må avveies mot andre rettigheter og friheter som gjør seg gjeldende, i henhold til proporsjonalitetsprinsippet i pakten artikkel 52. Som fremhevet av EU-domstolen i Schrems II-saken, er ikke retten til vern av personopplysninger en absolutt rettighet – den må vurderes opp mot sin funksjon i samfunnet.

En annen relevant faktor i en kontekstuell tolkning av GDPR, er dens fortale. I tråd med TEUV artikkel 296 annet ledd om at alle rettsakter må begrunnes, gir fortalen anvisning på forordningens formål. Som for alle EU-rettsakter er imidlertid ikke fortalen rettslig bindende,[44] og gir dermed kun tolkningsbidrag så fremt den ikke medfører en fortolkning i strid med en ellers klar ordlyd.[45]

[40] Fredriksen og Mathisen (2014) s. 21.
[41] Traktaten om Den europeiske union (TEU).
[42] Se forente saker C-402 og 432/07 *Sturgeon*, der EU-domstolen i avsnitt 47 legger til grunn som et generelt tolkningsprinsipp at «a Community act must be interpreted, as far as possible, in such a way as not to affect its validity».
[43] Fredriksen og Mathisen (2014) s. 225.
[44] C-7/11 *Caronna*, avsnitt 40.
[45] C-345/13 *Karen Millen Fashions*, avsnitt 31.

Ettersom GDPR trådte i kraft så sent som i 2018, er det en rekke aspekter ved den som ennå ikke er avklart i autoritative kilder. Da kan det være relevant å se hen til forordningens tilblivelseshistorie, som kan bidra til å bekrefte eller avkrefte forskjellige tolkningsalternativer.[46] Et eksempel er *Satakunnan Markkinapörssi*-saken[47], der EU-domstolen vurderte innholdet i det daværende personverndirektivet[48] artikkel 9, som ga unntak fra direktivets bestemmelser ved databehandling utført «utelukkende i journalistisk øyemed».[49] For sin tolkning viste EU-domstolen til «the legislative history of the directive», med videre henvisning til generaladvokatens innstilling, som fremhevet uttalelser fra Kommisjonen, Europaparlamentet og Rådet fra prosessen frem mot direktivets vedtakelse.[50] På tilsvarende måte vil GDPRs tilblivelseshistorie være relevant i forbindelse med oppgavens redegjørelse for den risikobaserte tilnærmingen i forordningen, herunder diskusjonene og rapportene som fant sted i reformprosessen fra personverndirektivet til GDPR. Dette kan illustrere hensikten bak forordningens utforming, som videre kan fungere som tolkningsbidrag for spørsmålet om den risikobaserte tilnærmingen også gjelder ved overføring til tredjestater.

I tillegg til GDPR og dens hjemmelsgrunnlag, står praksis fra EU-domstolen sentralt for oppgavens problemstilling. Domstolen skal ifølge TEU artikkel 19 nr. 1 «ensure that in the interpretation and application of the Treaties the law is observed», og er med dette tillagt en viktig oppgave fra medlemsstatene til å tolke EU-rettens nærmere innhold. Selv om dens avgjørelser som et utgangspunkt ikke har formelle prejudikatsvirkninger, er det derfor klart at de utgjør tungtveiende rettskilder.[51] Når det kommer til EU-domstolens avgjørelser i saker som er forelagt den fra en nasjonal domstol i henhold til TEUV artikkel 267 – prejudisielle avgjørelser – er disse bindende for alle nasjonale domstoler i den konkrete saken.[52] Schrems II-dommen er en prejudisiell avgjørelse.[53] I lys av det som er sagt om EU-domstolens rolle

[46] Fredriksen og Mathisen (2014) s. 228.
[47] C-73/07 *Satakunnan Markkinapörssi.*
[48] Direktiv 95/46/EF om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (Personverndirektivet).
[49] Fredriksen og Mathisen (2014) s. 229.
[50] Fredriksen og Mathisen (2014) s. 229, med videre henvisning til avsnitt 65 i generaladvokat Kokotts innstilling i saken.
[51] Fredriksen og Mathisen (2014) s. 238.
[52] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al14552 (sist lest 04.03.2021).
[53] I tråd med dette kom den irske High Court med sin endelige avgjørelse i saken den 14. mai 2021. Det irske datatilsynet ble her pålagt å håndheve kravene etter Schrems II-dommen, og stanse Facebook sine overføringer av personopplysninger fra Europa til USA. Se nærmere på https://noyb.eu/en/decision-irish-high-court-jr?fbclid=IwAR2ybDoEURYM2U4OoosL2YpatNS1kHoriweSJRYOYL2pyPhg-g36OHoNtBM (sist lest 21.mai 2021).

ved fortolkning av EU-retten er det imidlertid klart at denne avgjørelsen har stor betydning for overføring av personopplysninger til tredjestater generelt.

EU-domstolens avgjørelse i Schrems II-saken er den siste av flere anledninger der domstolen har tatt stilling til ulike problemstillinger som oppstår i forbindelse med overføring av personopplysninger til tredjestater.[54] Den har imidlertid ikke tatt eksplisitt stilling til betydningen av *risiko* i denne sammenheng. Det henger antakelig sammen med at EU-domstolen generelt sett er kortfattet og lite drøftende i stilen.[55] Dermed blir det nødvendig med en nærmere tolkning av Schrems II-dommens premisser, med sikte på å identifisere uttalelser som kan ha betydning for oppgavens problemstilling. Domstolens forsiktige stil – som dels kan henge sammen med forbudet mot offentlige dissenser – innebærer imidlertid at vidtgående slutninger fra dommenes premisser bør trekkes med varsomhet.[56]

Særlig relevant for oppgavens problemstilling er retningslinjer fra Personvernrådet, herunder det nevnte utkastet til retningslinjer vedrørende kravene til supplerende beskyttelsestiltak etter Schrems II-dommen.[57] Personvernrådet består av representanter fra tilsynsmyndighetene i samtlige av EUs medlemsland, samt EUs datatilsyn (European Data Protection Supervisor, heretter «EDPS» eller «EUs datatilsyn»), jf. GDPR artikkel 68 nr. 3. I tillegg består rådet av representanter fra EFTA-statene Norge, Island og Liechtenstein, men disse har ikke stemmerett.[58] Med det formål å sikre ensartet anvendelse av GDPR, skal Personvernrådet nettopp utstede retningslinjer, anbefalinger og beste praksis knyttet til anvendelsen av forordningen, jf. artikkel 70 nr. 1 bokstav e.

Det norske datatilsynet viser på sine nettsider til at Personvernrådets uttalelser har «stor rettskildemessig vekt», med henvisning til at de er hjemlet i GDPR, og at de gir uttrykk for en felles forståelse mellom datatilsynsmyndighetene på tvers av landegrensene i EU- og EØS-området.[59] På samme måte som for retningslinjer og anbefalinger ellers i EU-retten, er imidlertid ikke Personvernrådets uttalelser bindende, jf. TEUV artikkel 288 nr. 5. Selv om det i lys av det som er sagt er naturlig at nasjonale datatilsyn legger stor vekt på Personvernrådets

[54] Se nærmere om Schrems II-dommen under kapittel 5.
[55] Fredriksen og Mathisen (2014) s. 239.
[56] Fredriksen og Mathisen (2014) s. 239.
[57] EDPB Recommendations 01/2020. Veilederen er ikke endelig vedtatt på tidspunktet for innleveringen av denne oppgaven. Selv om dette er en kilde som står sentralt for oppgavens problemstilling, tas det derfor forbehold om at Personvernrådet kan gi uttrykk for en annen rettsoppfatning i veilederens endelige versjon.
[58] Personvernrådets sammensetning er tilgjengelig på https://edpb.europa.eu/about-edpb/about-edpb/members_en.
[59] Datatilsynet (2019).

retningslinjer, er det med andre ord klart at de må vike for bindende EU-rettslige kilder ved eventuell motstrid.

Før GDPR trådte i kraft var det for øvrig Artikkel 29-gruppen som utførte det som nå er Personvernrådets oppgaver. I forbindelse med omtalen av reformprosessen fra personverndirektivet frem mot vedtakelsen av GDPR, vil enkelte uttalelser fra Artikkel 29-gruppen være av relevans. Heller ikke disse uttalelsene er bindende, men er egnet til å illustrere en rekke sentrale poenger.

Hva gjelder de standardiserte personvernbestemmelsene som overføringsgrunnlag, har Kommisjonen fått kompetanse gjennom GDPR artikkel 46 nr. 2 bokstav c til å bestemme det nærmere innholdet i disse. Ettersom forpliktelsene i standardkontraktene er ment å være i tråd med prinsippene og reglene i GDPR om hvordan personopplysninger skal behandles,[60] har Kommisjonen fått delegert myndighet til å avgjøre hva som utgjør et tilstrekkelig beskyttelsesnivå. Vedtakelsen av personvernbestemmelsene er en kommisjonsbeslutning i medhold av TEUV artikkel 291 nr. 2, med den virkning at det er tale om en bindende rettsakt.

En særlig relevant og fersk kilde for oppgavens problemstilling er i forlengelsen av dette Kommisjonens forslag til nye standardiserte personvernbestemmelser.[61] Innholdet her kan si noe om Kommisjonens forståelse av EU-domstolens krav om supplerende beskyttelsestiltak i Schrems II-dommen.[62] Kommisjonens tolkning av dette kravet har naturligvis begrenset vekt i forhold til GDPR, pakten om grunnleggende rettigheter og EU-domstolens uttalelser, men kan på lik linje med Personvernrådets anbefalinger tale for eller imot ulike tolkningsalternativer. En forskjell fra Personvernrådets anbefalinger er imidlertid at utformingen av de standardiserte personvernbestemmelsene har langt større praktisk betydning. Selv om Personvernrådets anbefalinger er en viktig rettskilde i praksis, følger det av deres manglende bindende evne at de kan fravikes. Vilkårene i de standardiserte personvernbestemmelsene må derimot følges dersom disse bestemmelsene i det hele tatt kan tas i bruk som overføringsgrunnlag. Innholdet her vil med andre ord gi anvisning på hvordan kravene til

[60] Jarbekk mfl. (2019) s. 375.
[61] Draft implementing decision (2020).
[62] Den 4. juni 2021 vedtok Kommisjonen en endelig versjon av de nye standardiserte personvernbestemmelsene (Commission Implementing Decision (2021) – tilgjengelig her: https://ec.europa.eu/info/sites/default/files/1_en_act_part1_v5.pdf). Ettersom vedtaket kom tre dager før innleveringen av denne oppgaven, behandles ikke denne versjonen nærmere her (se neste punkt om avgrensninger). Det kan imidlertid bemerkes at delene av kommisjonsutkastet som behandles under punkt 7.2 i oppgaven, ikke er vesentlig endret i Kommisjonens endelige vedtak. Se særlig fotnote 190 i denne oppgaven om dette.

supplerende beskyttelsestiltak i praksis vil følges, helt til de eventuelt utfordres for EU-domstolen.

Avgjørelser og uttalelser fra nasjonale tilsynsmyndigheter opprettet i medhold av GDPR artikkel 51 kan også være av relevans når forordningen fortolkes. Disse avgjørelsene og uttalelsene har begrenset rettskildemessig vekt, men er egnet til å illustrere hvordan ulike bestemmelser i forordningen er tolket på nasjonalt nivå. Det samme gjelder praksis fra nasjonale domstoler i EU og EØS.

Til slutt vil det også vises til juridisk litteratur og rapporter fra diverse forskningsinstitusjoner. Heller ikke dette er kilder av nevneverdig vekt, men de er etter forholdene godt egnet til å gi økt forståelse for de øvrige rettskildenes innhold og praktiske betydning.

Som følge av at oppgaven baserer seg på relativt ferske kilder, byr skriveprosessen på en rekke rettskildemessige utfordringer. Ettersom GDPR trådte i kraft i 2018, og Schrems II-dommen ble avsagt i juli i 2020, er omfanget av øvrige kilder som bidrar til forståelsen av deres innhold begrenset. Dertil kommer at nye kilder strømmer til underveis i skriveprosessen, potensielt også etter at store deler av struktur og innhold er satt. Dette innebærer at vi hele veien må holde øynene åpne for kilder som kan være av relevans, samtidig som vi på et nokså tidlig stadium må avgjøre hvilke kilder som skal danne hovedgrunnlaget for analysen.

## 1.4 Avgrensninger

For å kunne gi en samvittighetsfull og grundig analyse av de sentrale rettskildene for oppgavens problemstilling, er det nødvendig med en tidsmessig grense for når nye kilder kan hensyntas. I samråd med veileder er det derfor bestemt at oppgaven kun vil ta utgangspunkt i det rettskildebildet som eksisterer per 31. mai 2021.

Videre aktualiserer tematikken rundt overføring av personopplysninger til tredjestater en rekke underproblemstillinger. Samtidig nødvendiggjør oppgavens problemstilling et dypdykk i personvernforordningen, samt en gjennomgang av andre relevante rettskilder. For å kunne gjøre dette dypdykket, må det avgrenses mot en rekke av disse underproblemstillingene.

Overføring av personopplysninger til tredjestater kan skje på grunnlag av en rekke forskjellige bestemmelser. For det første kan overføringen finne sted der EU-kommisjonen har gitt en

beslutning om at mottakerstaten sikrer et tilstrekkelig beskyttelsesnivå, jf. artikkel 45 nr. 1 i GDPR. I skrivende stund har Kommisjonen gitt en slik beslutning for Andorra, Argentina, Canada, Færøyene, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Sveits og Uruguay.[63] Tilsvarende beslutninger er også ventet å komme for Storbritannia, som i kjølvannet av Brexit er å anse som en tredjestat, samt Sør-Korea.[64]

Dersom Kommisjonen ikke har gitt en slik beslutning for den aktuelle mottakerstaten, kan overføringen likevel skje dersom eksportøren gir «nødvendige garantier» og de registrerte har «håndhevbare rettigheter og effektive rettsmidler», jf. artikkel 46 nr. 1 i GDPR. Slike garantier kan i medhold av artikkel 46 nr. 2 i første rekke gis gjennom et rettslig bindende og håndhevbart instrument mellom offentlige myndigheter eller organer, jf. bokstav a, bindende virksomhetsregler i samsvar med artikkel 47, jf. bokstav b, standard personvernbestemmelser vedtatt av Kommisjonen, jf. bokstav c, standard personvernbestemmelser vedtatt av en tilsynsmyndighet og godkjent av Kommisjonen, jf. bokstav d, godkjente atferdsnormer i henhold til artikkel 40, jf. bokstav e, eller en godkjent sertifiseringsmekanisme i henhold til artikkel 42, jf. bokstav f. Etter godkjenning fra tilsynsmyndigheten i medhold av artikkel 46 nr. 3, kan nødvendige garantier også gis gjennom avtalevilkår mellom eksportøren og importøren av personopplysningene, eller ved administrative ordninger mellom offentlige myndigheter og organer, jf. henholdsvis bokstav a og b. Dersom det verken foreligger en adekvansbeslutning fra Kommisjonen etter artikkel 45, eller det er gitt nødvendige garantier etter artikkel 46, kan overføring av personopplysninger til en tredjestat finne sted på grunnlag av rettslige avgjørelser avsagt av domstoler eller administrative myndigheter, forutsatt at avgjørelsene bygger på en internasjonal avtale, jf. artikkel 48. Helt unntaksvis kan overføringen også skje på grunnlag av samtykke- eller nødvendighetsbetraktninger i medhold av artikkel 49.[65]

Ettersom avtaler basert på de standardiserte personvernbestemmelsene vedtatt av Kommisjonen etter artikkel 46 nr. 2 bokstav c i GDPR kan inngås av alle virksomheter, og ikke krever videre godkjenning fra offentlige instanser, er dette det mest praktiske overføringsgrunnlaget. De standardiserte personvernbestemmelsene brukes av om lag 85 %

[63] Kommisjonens adekvansbeslutninger er tilgjengelig på https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (sist lest 26.05.2021).
[64] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (sist lest 26.05.2021).
[65] EDPB Guidelines 2/2018 s. 4. Personvernrådet uttaler at unntaksadgangen her skal tolkes strengt.

av europeiske bedrifter,[66] og var et av hovedtemaene i Schrems II-saken. Derfor er det dette overføringsgrunnlaget som vil stå i fokus i oppgaven, med den konsekvens at det ikke vil foretas en nærmere gjennomgang av *øvrige overføringsgrunnlag* i GDPR kapittel V. Likevel vil EU-domstolens begrunnelse for kravet om supplerende beskyttelsestiltak ved bruk av standardiserte personvernbestemmelser – at myndighetene i mottakerstaten ikke er bundet av de garantier og forpliktelser som dette overføringsgrunnlaget fører med seg – gjøre seg gjeldende for de øvrige overføringsgrunnlagene som er av kontraktsrettslig natur. Dette fremheves av både EU-domstolen i Schrems II-dommen,[67] og av Personvernrådets veileder om supplerende beskyttelsestiltak.[68] Analysen i denne oppgaven vil derfor langt på vei være relevant for øvrige overføringsgrunnlag etter GDPR artikkel 46.

For å avgjøre hvilke beskyttelsestiltak som er påkrevd ved den enkelte overføring, må det først foretas en vurdering av beskyttelsesnivået i den konkrete mottakerstaten. I forbindelse med denne *landrisikovurderingen* har Personvernrådet publisert en særskilt veileder, som gir anvisning på hvilke elementer som er sentrale ved vurderingen av beskyttelsesnivået.[69] Her fremheves særlig mottakerstatens overvåkningslovgivning som en sentral kilde som må vurderes. Rimeligheten ved omfattende krav til eksportøren av personopplysningene om å foreta slike landrisikovurderinger kan diskuteres, blant annet fordi slike vurderinger innebærer at eksportøren av personopplysningene må foreta svært kompliserte og ressurskrevende undersøkelser. Det vises i denne sammenheng til at nasjonal overvåkningslovgivning ofte er klassifisert eller utilgjengelig.[70] Utfordringene med et slikt krav illustreres også av at Kommisjonens egne landrisikovurderinger av USA har blitt underkjent to ganger, jf. EU-domstolens avgjørelser i Schrems I- og Schrems II-sakene. Som fremhevet av Theodore Christakis, er kravene i veilederen tilknyttet landrisikovurderingen i tillegg såpass strenge at de fleste land nok uansett ikke vil bestå den.[71]

Kritikken rettet mot Personvernrådets krav tilknyttet denne vurderingen dreier seg med andre ord dels om problemer som i første rekke er av teknisk karakter, og dels om at det stilles

[66] Digital Europe (2020) s. 5.
[67] C-311/18 *Schrems II,* avsnitt 132.
[68] EDPB Recommendations 01/2020 s. 18, avsnitt 58.
[69] EDPB Recommendations 02/2020.
[70] Rubinstein og Margulies (2021) s. 23. I artikkelen vises det til en rapport som gjennomgår overvåkningslovgivningen i 12 ulike stater. Her ble det funnet at overvåkningslovgivningen gjerne var klassifisert eller utilgjengelig, og at statens praksis ofte ikke samsvarte med det som fremgikk av lovgivningen.
[71] Christakis (2020) del 2. Han viser her til at også praksisen i europeiske stater står i faresonen ut fra Personvernrådets krav.

urealistiske krav til myndigheters overvåkningspraksis. Selv om landrisikovurderingen naturligvis henger tett sammen med kravet om supplerende beskyttelsestiltak, all den tid den legger grunnlaget for hvilke personvernrettslige hull som må tettes i den konkrete saken, går kritikken derfor utenfor det som skal behandles i oppgaven. Utover spørsmålet om *sannsynligheten* for at tredjestatens myndigheter vil kreve innsyn i de overførte personopplysningene er en relevant faktor, vil derfor ikke Personvernrådets krav tilknyttet landrisikovurderingen, herunder den særskilte veilederen om dette, gjøres nærmere rede for.[72]

En annen problemstilling knytter seg til hvilke tilfeller kravene etter Schrems II-saken gjelder. Oppfatningen har vært at reglene om overføring av personopplysninger til tredjestater kun gjelder der personopplysningene overføres til en adresse i en tredjestat.[73] Konsekvensen av det er at dersom et amerikansk selskap tilbyr lagring på servere i et EU-land, og forplikter seg til å kun bruke disse serverne, gjør ikke kravene i GDPR kapittel V seg gjeldende.[74] Imidlertid er begrunnelsen for EU-domstolens krav om supplerende beskyttelsestiltak nettopp at slike kontraktsrettslige forpliktelser ikke er bindende for tredjestatens myndigheter. Denne begrunnelsen gjør seg også gjeldende der tjenesteleverandøren opererer i Europa, men er underlagt en tredjestats overvåkningslovgivning. Det kan eksempelvis tenkes at en EU-basert skytjenesteleverandør instrueres av sitt amerikanske morselskap om å overføre et gitt sett med personopplysninger, etter pålegg fra amerikanske overvåkningsmyndigheter. I en slik situasjon vil skytjenesteleverandøren måtte velge mellom å bryte sine kontraktsrettslige forpliktelser overfor oppdragsgiver, eller å gå imot myndighetenes pålegg. Problemstillingen som oppstår i forlengelsen av dette er hvilke implikasjoner EU-domstolens begrunnelse i Schrems II-saken har for disse tilfellene, herunder om kravet om supplerende beskyttelsestiltak gjør seg like mye gjeldende her.[75] Oppgavens fokus er imidlertid *innholdet* i kravet om supplerende beskyttelsestiltak, og ikke kravets anvendelsesområde. Det avgrenses derfor mot en nærmere diskusjon rundt denne problemstillingen.

---

[72] Det kan også nevnes at EU-domstolen kort tid etter Schrems II-avgjørelsen avsa dom i C-623/17 *Privacy International* og C-511/18 *La Quadrature du Net and Others*, der domstolen tok stilling til overvåkningsmyndigheters adgang til å pålegge tilbydere av kommunikasjonstjenester å utlevere kommunikasjonsdata. Kravene som stilles her står sentralt ved vurderingen av om en potensiell mottakerstat for overføring av personopplysninger har et adekvat beskyttelsesnivå.

[73] Wessel-Aas og Ødegaard (2018) s. 245.

[74] Wessel-Aas og Ødegaard (2018) s. 245.

[75] I en sak mellom det franske helsedirektoratet og Interhop med flere anvendte den høyeste administrative domstolen i Frankrike (Conseil d'État) kravene etter Schrems II-dommen på et tilfelle hvor opplysningene ble oppbevart innenfor EU/EØS, men av et amerikanskeid selskap. Saken gjennomgås nærmere i punkt 6.3.

GDPR er innlemmet i EØS-avtalen, og får derfor anvendelse i EFTA-statene Norge, Island og Liechtenstein i tillegg til EUs medlemsstater.[76] Et relevant spørsmål i kjølvannet av EU-domstolens avgjørelse i Schrems II-saken er hvilke konsekvenser den får for EFTA-pilaren i EØS-samarbeidet. Det er ikke gitt at EU-domstolens ugyldiggjøring av Privacy Shield-ordningen er bindende for EFTA-statene.[77] Det kan i denne sammenhengen vises til at EU-domstolens ugyldiggjøring av Privacy Shield i hovedsak bygger på at ordningen ikke var kompatibel med EUs pakt om grunnleggende rettigheter – en rettskilde som verken er innlemmet i EØS-avtalen eller på annen måte er formelt anerkjent av partene i EØS-avtalen.[78] Oppgaven tar imidlertid kun sikte på å analysere gjeldende EU-rett. Særskilte EØS-rettslige problemstillinger vil derfor ikke tas stilling til her.

## 1.5 Fremstillingen videre

For å gi oversikt over oppgavens tema, vil det i kapittel 2 av oppgaven forklares hva som menes med en *risikobasert tilnærming* ved behandling av personopplysninger. I denne sammenheng vil den risikobaserte tilnærmingen sammenlignes med sitt motstykke i den rettighetsbaserte tilnærmingen i punkt 2.1. Formålet med denne sammenligningen er å danne grunnlag for en nærmere forståelse av hvordan valg av tilnærming påvirker utpenslingen av Schrems II-dommens krav om supplerende beskyttelsestiltak. Derfor vil det i punkt 2.2 presenteres en rekke eksempler på aktuelle beskyttelsestiltak som typisk vil måtte kreves etter de to tilnærmingene.

For å ta stilling til oppgavens problemstilling, må det foretas en nærmere gjennomgang og analyse av de relevante personvernrettslige reglene i EU. Selv om Schrems II-dommen, Personvernrådets veileder og Kommisjonens forslag til nye standardiserte personvernbestemmelser ligger nærmest problemstillingen i tid og innhold, er det først nødvendig med en gjennomgang av de viktigste bakenforliggende rettskildene. Oppgavens primære rettskilde er som nevnt GDPR, som igjen må tolkes i overenstemmelse med EUs pakt om grunnleggende rettigheter. De tolkningsbidrag som presenteres av EU-domstolen, Personvernrådet og Kommisjonen i relasjon til spørsmål om supplerende beskyttelsestiltak

[76] Regjeringen (2014).
[77] Problemstillingen er nærmere drøftet her: https://rett24.no/articles/hva-om-privacy-shield-fortsatt-lever-i-norge-island-og-liechtenstein (sist lest 06.05.2021).
[78] Fredriksen (2013) s. 371.

ved overføring av personopplysninger til tredjestater bygger derfor på innholdet i nettopp GDPR og pakten. Følgelig må de to sistnevnte rettskildene behandles først.

I kapittel 3 av oppgaven vil det derfor gjøres grundig rede for hva GDPR sier om risiko, med sikte på å identifisere hvorvidt forordningen legger til rette for en risikobasert tilnærming også ved overføring av personopplysninger til tredjestater. Risiko spiller en fremtredende rolle i forordningens kapittel IV, noe som har sin forklaring i det såkalte ansvarsprinsippet. Før det gis en gjennomgang av de risikobaserte bestemmelsene i GDPR kapittel IV i punkt 3.3, vil derfor ansvarsprinsippet presenteres i punkt 3.2. Deretter vil forordningens utforming og funksjon som en såkalt meta-regulering analyseres i punkt 3.4. Denne analysen skal danne grunnlag for en nærmere forståelse av rasjonalet bak systemet i GDPR, og dermed også sammenhengen mellom ansvarsprinsippet og den risikobaserte tilnærmingen.

Etter denne analysen av GDPR som meta-regulering vil det foretas en gjennomgang av de relevante bestemmelsene i forordningens kapittel V om overføring av personopplysninger til tredjestater. Her er formålet å identifisere elementer i dette kapittelet som kan si noe om i hvilken grad den risikobaserte tilnærmingen i kapittel IV har betydning ved overføringer til tredjestater, eller om en slik tilnærming ikke er like relevant her.

Av hensyn til grunnrettighetspaktens sentrale posisjon for oppgavens problemstilling, vil det deretter i kapittel 4 vurderes hvilken betydning denne kan ha for relevansen av risikovurderinger ved overføring av personopplysninger til tredjestater. Vurderingen vil særlig ta utgangspunkt i friheten til å opprette og drive egen forretningsvirksomhet i pakten artikkel 16, sammenholdt med proporsjonalitetsprinsippet i artikkel 52. Spørsmålet her er nærmere bestemt hvorvidt det kreves en risikobasert tilnærming til kravet om supplerende beskyttelsestiltak for at inngrepet i friheten til å drive forretningsvirksomhet skal være proporsjonalt.

Etter å ha gjennomgått sentrale regler i det personvernrettslige regelverket, er det relevant med en nærmere gjennomgang av Schrems II-dommen i kapittel 5 av oppgaven. Som det fremgikk av punkt 1.1 og 1.2, gir ikke dommen eksplisitt svar på om den konkrete risikoen ved overføringen er en relevant faktor ved kravet om supplerende beskyttelsestiltak. Imidlertid kan dommens premisser undergis en nærmere analyse, med sikte på å identifisere visse sammenhenger og beveggrunner som kan gi indikasjoner i den ene eller andre retningen om EU-domstolens tilnærming til risiko. En slik analyse foretas i punkt 5.3. Først vil det

imidlertid i punkt 5.2 gjøres grundig rede for domstolens begrunnelse for kravet om supplerende beskyttelsestiltak, som et grunnlag for analysen.

I forlengelsen av analysen av Schrems II-dommen, vil det i kapittel 6 foretas en gjennomgang av Personvernrådets veileder knyttet til dommens krav om supplerende beskyttelsestiltak. Deretter vil det ses hen til Kommisjonens utkast til nye standardiserte personvernbestemmelser i kapittel 7, for å vurdere hvilken tilnærming Kommisjonen har til EU-domstolens krav.

Med utgangspunkt i de nevnte kildene, vil det i kapittel 8 fattes en konklusjon på problemstillingen om en risikobasert tilnærming ved overføring av personopplysninger til tredjestater. I punkt 8.1 sammenfattes de vurderinger og analyser som er foretatt i oppgaven, før det konkluderes på spørsmålet om risiko i det hele tatt er relevant ved utpenslingen av Schrems II-dommens krav om supplerende beskyttelsestiltak. Deretter vil oppgavens punkt 8.2 belyse hvilke praktiske konsekvenser en potensiell risikobasert tilnærming har for bedrifters oppfyllelse av dette kravet ved overføringer ut av EU/EØS.

Avslutningsvis vil det i kapittel 9 vies plass til noen avsluttende betraktninger om Schrems II-dommens og oppgavens underliggende problem, nærmere bestemt den vanskelige balansegangen mellom personvernet og den teknologiske utviklingen. I denne sammenheng vil det knyttes noen tanker til hvilke potensielle løsninger vi kan se for oss på kort og lang sikt, som kan gjøre denne balansegangen lettere. Her vil lovgivingsteknikk (punkt 9.2) og teknologiselskapenes innovasjon (punkt 9.3) stå i fokus, før det med utgangspunkt i det som er sagt drøftes rundt den mulige veien videre (punkt 9.4).

# 2 Risikobasert tilnærming contra rettighetsbasert tilnærming

## 2.1 Nærmere om begrepene *risiko* og *risikobasert tilnærming*

Ordet *risiko* er ikke eksplisitt definert i GDPR, men nevnes i en rekke bestemmelser (se nærmere under punkt 3.3), der det gis anvisning på en vurdering av «risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter», jf. eksempelvis artikkel 24. En naturlig språklig forståelse av ordlyden her peker på risiko som muligheten for ulike skadelige konsekvenser for de registrertes rettigheter og friheter som følge av databehandlingen. Dette kan igjen forstås som en kombinasjon av *alvorlighetsgraden* av skaden på de registrertes rettigheter og friheter, og *sannsynligheten* for at skaden vil inntreffe.[79] I forlengelsen av dette vises det i fortalepunkt 75 til en rekke potensielle fysiske, materielle eller ikke-materielle skader det må tas hensyn til.

Dersom den konkrete risikoen for myndighetsinnsyn er relevant for spørsmålet om hvilke supplerende beskyttelsestiltak som er egnede ved overføring av personopplysninger til tredjestater, må det med andre ord tas stilling til *sannsynligheten* for at tredjestatens myndigheter begjærer innsyn i de aktuelle personopplysningene, samt de potensielle *konsekvensene* av en slik innsynsbegjæring.

Begrepet *risikobasert tilnærming* ble introdusert i debatten rundt reformen fra personverndirektivet til personvernforordningen. Fokuset på risiko er nemlig et av de mest sentrale elementene som skiller forordningen fra personverndirektivet. Der direktivet i stor grad benyttet forhåndskontroll og tilsynsgodkjenning, er det den behandlingsansvarliges

[79] En slik forståelse av risiko er i tråd med digitaliseringsdirektoratet sin definisjon: «Risiko handler om potensielle avvik fra det forventede eller potensielle avvik fra våre mål. Med det referansepunktet defineres risiko formelt som en kombinasjon av mulige konsekvenser (utfall eller resultat) og tilhørende usikkerhet. Usikkerheten kvantifiseres ved hjelp av sannsynligheter. […] [R]isiko er kombinasjonen av (mulige) konsekvenser og (tilhørende) sannsynligheter, eller bare at risiko er kombinasjonen av konsekvens og sannsynlighet», se https://internkontroll-infosikkerhet.difi.no/risikostyring/hva-er-risiko (sist lest 15.03.2021). Denne definisjonen baserer seg på den internasjonale definisjonen i ISO Guide 73:2009, som benyttes i ISO/IEC 27001 og på https://snl.no/risiko (sist lest 15.03.2021).

risikovurderinger som nå benyttes som den sentrale mekanismen for å etterleve forordningens krav.[80] I hovedsak innebærer den risikobaserte tilnærmingen å regulere graden av beskyttelse personopplysningene har ut ifra hvor stor risiko den enkelte databehandlingen innebærer for de registrertes rettigheter.[81] Ved overføring av personopplysninger til tredjestater, vil en slik tilnærming blant annet innebære at kravene til beskyttelsestiltak varierer med sannsynligheten for og konsekvensene av en innsynsbegjæring fra myndighetene.

Motsatsen til risikobasert tilnærming er *rettighetsbasert tilnærming.* Tradisjonelt sett gir en slik tilnærming lite rom for å nedskalere beskyttelsen med utgangspunkt i en risikoanalyse. Grovt skissert tar den rettighetsbaserte tilnærmingen utgangspunkt i om de aktuelle kravene er oppfylt ut fra et rettslig perspektiv – enten er en gitt aktivitet lovlig eller ulovlig.[82] I relasjon til GDPR vil dette innebære at de samme reglene og det samme rammeverket implementeres for enhver databehandlingsaktivitet, uavhengig av risikoen for at rettigheter krenkes.[83] En slik tilnærming vil følgelig sikre et «minimum and non-negotiable level of protection for all individuals».[84]

I forbindelse med en eventuell overføring til en tredjestat, innebærer en rettighetsbasert tilnærming at beskyttelsestiltakene *fullt ut* må sikre at de registrertes rettigheter etter forordningen ikke krenkes. Nærmere bestemt må de standardiserte personvernbestemmelsene, sammenholdt med de supplerende beskyttelsestiltakene, gjøre det tilnærmet umulig for tredjestatens myndigheter å få tilgang til de aktuelle personopplysningene, uavhengig av den konkrete risikoen. Eksempelvis vil en overføring av helt enkle kontaktopplysninger som uansett ligger tilgjengelig på internett, og som sannsynligvis verken vil være gjenstand for en innsynsbegjæring fra tredjestatens myndigheter eller vil innebære nevneverdige konsekvenser for den registrerte dersom innsyn finner sted, ikke kunne skje uten full beskyttelse. Sammenlignet med en risikobasert tilnærming gir en rettighetsbasert tilnærming med andre ord langt mindre fleksibilitet for virksomheter som overfører eller planlegger å overføre personopplysninger til tredjestater.

[80] Gonçalves (2019) s. 139-152. Gonçalves nevner i artikkelens note 7: «Note that the term «risk» appears 76 times in the text of the Regulation, whereas it appeared 8 times in the text of the Directive». Se også fortalepunkt 89 til GDPR.
[81] Kuner, Bygrave og Docksey (2020) s. 26.
[82] Gellert (2020) s. 2.
[83] Lynskey (2016) s. 35-40.
[84] Art 29 WP, Opinion 1/98 s. 2.

## 2.2 Eksempler på tilnærmingens betydning for kravet om supplerende beskyttelsestiltak

Spørsmålet om hvilke beskyttelsestiltak som gir tilstrekkelig beskyttelse ved overføring av personopplysninger til tredjestater, vil etter dette avhenge av om man inntar en rettighetsbasert eller en risikobasert tilnærming.

Med en ren rettighetsbasert tilnærming til spørsmålet, vil det i realiteten alltid være nødvendig med tekniske tiltak. Som nevnt innledningsvis under punkt 1.1, er poenget i Schrems II-dommen at de kontraktsrettslige forpliktelsene som følger av EUs standardiserte personvernbestemmelser, ikke er bindende for tredjestatens myndigheter. Dette poenget gjør seg naturligvis også gjeldende for eventuelle supplerende kontraktsrettslige og organisatoriske tiltak, med den konsekvens at det kun er nettopp tekniske tiltak som kan forhindre innsyn fra de aktuelle myndighetene.[85]

Et aktuelt og nærliggende teknisk tiltak mot innsyn fra tredjestatens myndigheter er *kryptering*. Kryptering er av Datatilsynet definert som «en matematisk metode som sørger for konfidensialitet ved at informasjonen ikke kan leses av uvedkommende».[86] Når en tekst krypteres, omformes den fra klartekst til en rad med tilfeldige tegn.[87] For å få tilgang til informasjonen, må man ha en såkalt krypteringsnøkkel, som er en algoritme som gjør teksten lesbar igjen.[88] Selv om de aktuelle personopplysningene er kryptert, vil det med en rettighetsbasert tilnærming ikke være tilstrekkelig beskyttelse så lenge mottakeren av opplysningene i tredjestaten sitter på krypteringsnøkkelen, all den tid vedkommende vil kunne bli pålagt av myndighetene å dekryptere de aktuelle personopplysningene. Etter en slik tilnærming må det med andre ord også være et krav at krypteringsnøkkelen forblir i EU/EØS.

Et annet potensielt effektivt tiltak er å *pseudonymisere* personopplysningene. Etter GDPR artikkel 4 nr. 5 innebærer «pseudonymisering» en behandlingsmåte der «personopplysningene ikke lenger kan knyttes til en bestemt registrert uten bruk av tilleggsopplysninger, forutsatt at nevnte tilleggsopplysninger lagres atskilt og omfattes av tekniske og organisatoriske tiltak som sikrer at personopplysningene ikke kan knyttes til en identifisert eller identifiserbar

[85] Denne implikasjonen av EU-domstolens begrunnelse i Schrems II-saken fremheves også av EUs personvernråd i EDPB Recommendations 01/2020. Se nærmere under punkt 6.2.
[86] Datatilsynet (2017).
[87] Wessel-Aas og Ødegaard (2018) s. 221.
[88] Wessel-Aas og Ødegaard (2018) s. 221.

person». Eksempelvis kan navnet til den aktuelle bedriftens kunde erstattes med et løpenummer før overføringen, mens resten av kundedataene forblir uendret.[89] Pseudonymisering vil ofte gjøres *ved hjelp av* kryptering, i den forstand at det er krypteringen som gjør informasjonen ugjenkjennelig.[90] Med en rettighetsbasert tilnærming til reglene i GDPR ved overføring av personopplysninger til tredjestater, kan overføringen være lovlig dersom det ikke er mulig for uvedkommende å skaffe personopplysningene i klartekst.

Ut fra hva som har fremgått om den risikobaserte tilnærmingen, er derimot ikke formålet med en slik tilnærming at beskyttelsestiltakene til enhver tid skal fullt ut skal beskytte personopplysningene mot innsyn fra tredjestatens myndigheter. Her dreier det seg snarere om å *redusere* risikoen for slikt innsyn til et tilfredsstillende nivå. Dette kan eksempelvis gjøres med kontraktsrettslige og organisatoriske tiltak, eller med krypteringsløsninger der mottakeren av personopplysningene får hånd om krypteringsnøkkelen i forbindelse med utførelsen av databehandlingsoppdraget.

[89] Jarbekk mfl. (2019) s. 121.
[90] Jarbekk mfl. (2019) s. 121.

# 3 Hva sier GDPR om risikoens betydning ved overføring av personopplysninger til tredjestater?

## 3.1 Overordnet

Som nevnt under punkt 2.1, har overgangen fra personverndirektivet til personvernforordningen ført med seg et økt fokus på risikobetraktninger. Dette kommer først og fremst til uttrykk i forordningens kapittel IV, som stiller en rekke krav til både behandlingsansvarlige og databehandlere. Med behandlingsansvarlige menes fysiske eller juridiske personer som «bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes», jf. artikkel 4 nr. 7, mens databehandlere er fysiske eller juridiske personer som «behandler personopplysninger på vegne av den behandlingsansvarlige», jf. artikkel 4 nr. 8 (egen understreking).

Bestemmelsene i kapittel IV innebærer blant annet at disse aktørene gjennomgående må foreta risikovurderinger ved befatning med personopplysninger. Dette må forstås i lys av at en rekke av kapittelets bestemmelser langt på vei konkretiserer det såkalte ansvarsprinsippet, som fremgår av artikkel 5 nr. 2, og som tillegger den behandlingsansvarlige et ansvar for overholdelse av personvernprinsippene i artikkel 5 nr. 1.

I det følgende vil det redegjøres for hvordan den risikobaserte tilnærmingen kommer til uttrykk i GDPR, og betydningen ansvarsprinsippet har for tilnærmingens tilstedeværelse i forordningen. I denne sammenheng vil ansvarsprinsippet forklares kort i punkt 3.2, før det gis en nærmere presentasjon av de risikobaserte bestemmelsene i forordningens kapittel IV i punkt 3.3. For å få en nærmere forståelse av sammenhengen mellom ansvarsprinsippet og den risikobaserte tilnærmingen, er det deretter nødvendig med en gjennomgang av GDPRs oppbygning og funksjon som en såkalt meta-regulering i punkt 3.4. Til slutt vil det i punkt 3.5 og 3.6 drøftes hvorvidt forordningens kapittel V om overføring av personopplysninger til tredjestater åpner for en risikobasert tilnærming ved slike overføringer, eller om risikobestemmelsene i kapittel IV må holdes atskilt herfra.

## 3.2 Ansvarsprinsippet

I GDPR artikkel 5 nr. 1 fremgår en rekke grunnleggende prinsipper for behandling av personopplysninger, herunder prinsippet om lovlighet, rettferdighet og åpenhet i bokstav a, formålsbegrensningsprinsippet i bokstav b, dataminimeringsprinsippet i bokstav c, riktighetsprinsippet i bokstav d, lagringsbegrensningsprinsippet i bokstav e og prinsippet om integritet og konfidensialitet i bokstav f. Disse prinsippene er sentrale for forståelsen av de øvrige reglene i forordningen, og må tas hensyn til både før, under og etter databehandlingen.[91] Dersom disse prinsippene overholdes er presumsjonen at de registrertes rettigheter etter GDPR også er ivaretatt.[92]

Viktigst for oppgavens problemstilling er imidlertid ansvarsprinsippet, som fremgår av artikkel 5 nr. 2 i GDPR. Her fremgår det at den behandlingsansvarlige er «ansvarlig for og skal kunne påvise at nr. 1 overholdes». Ansvarsprinsippet er todelt. For det første innebærer prinsippet at den behandlingsansvarlige virksomheten skal være proaktiv og organisere seg på en måte som gjør at personvernprinsippene etterleves.[93] Vedkommende virksomhet får her et større *ansvar* enn det som var tilfellet etter personverndirektivet, ved at den i større grad selv må vurdere hvorvidt databehandlingen er i samsvar med GDPR. Dette har gitt utslag i en rekke mer konkrete plikter som påhviler den behandlingsansvarlige og etter forholdene også databehandleren, og som fremgår av forordningens kapittel IV. Et sentralt element ved disse pliktene er risikovurderingene virksomhetene må foreta i forbindelse med de enkelte databehandlingsaktivitetene.

For det andre innebærer ansvarsprinsippet at den behandlingsansvarlige må kunne dokumentere etterlevelsen av GDPR. Ettersom en rekke viktige risikovurderinger overlates til den behandlingsansvarlige, må vedkommende virksomhet kunne etterprøve de vurderinger som er foretatt, og hva man har gjort for å redusere den aktuelle risikoen.[94]

Ansvarsprinsippet gjelder generelt i GDPR, også ved overføringer til tredjestater. Det kan i denne sammenheng vises til punkt 108 i forordningens fortale, som i relasjon til overføringer til tredjestater etter «nødvendige garantier» i artikkel 46, presiserer at «garantiene bør særlig omfatte samsvar med de allmenne prinsippene om behandling av personopplysninger».

[91] Wessel-Aas og Ødegaard (2018) s. 128-129.
[92] Skullerud mfl. (2018) s. 176.
[93] Skullerud mfl. (2018) s. 172.
[94] Skullerud mfl. (2018) s. 176.

Uttalelsene her må antakelig forstås som en henvisning til prinsippene i GDPR artikkel 5, herunder ansvarsprinsippet i bestemmelsens andre ledd.[95]

## 3.3 Risikobestemmelsene i GDPR kapittel IV

For å ivareta fysiske personers rettigheter, stiller kapittel IV i personvernforordningen krav overfor både behandlingsansvarlig og databehandler til å gjennomføre systematiske tiltak for å sikre informasjonens konfidensialitet, integritet og tilgjengelighet. Disse kravene fremgår av ulike bestemmelser om blant annet internkontroll og dokumentasjon av alle behandlinger i en virksomhet, gjennomføring av risikovurderinger, avvikshåndtering og krav til behandlingsansvarlig ved valg av databehandler. De tekniske og organisatoriske tiltakene som bestemmelsene gir anvisning på, skal sikre en effektiv gjennomføring av prinsippene for vern av personopplysninger, herunder prinsippene som listes opp i forordningen artikkel 5 nr. 1.[96] Kravene konkretiserer i så måte ansvarsprinsippet nevnt under forrige punkt, ved at de gir nærmere anvisning på hvordan den behandlingsansvarliges ansvar skal utøves. Felles for en rekke av forpliktelsene etter GDPR kapittel IV er at de henviser til risikovurderinger ved fastsettelsen av hvilke tiltak som kreves i forbindelse med den konkrete databehandlingen. For å belyse den risikobaserte tilnærmingen i dette kapittelet, vil et utvalg bestemmelser herfra presenteres i det følgende.

Artikkel 24 og 32 gir anvisning på kravene til henholdsvis internkontroll og informasjonssikkerhet. Skillet mellom disse er ikke helt skarpt – internkontroll er alle systematiske tiltak for å oppfylle regelverkets krav, mens informasjonssikkerhet er systematiske tiltak for å sikre informasjonens konfidensialitet, integritet og tilgjengelighet. Mange av tiltakene vil derfor naturligvis falle inn under begge kategoriene.[97] I artikkel 24 pålegges den behandlingsansvarlige å gjennomføre «egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar» med GDPR. I vurderingen av hva som anses som *egnet*, skal det blant annet tas hensyn til «risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter». Tilsvarende i artikkel 32, som pålegger både den behandlingsansvarlige og databehandleren å gjennomføre «egnede» sikkerhetstiltak ut fra blant annet en risikovurdering. I bestemmelsens

[95] Kuner, Bygrave og Docksey (2020) s. 803.
[96] Skullerud mfl. (2018) s. 281.
[97] Skullerud mfl. (2018) s. 170.

andre ledd presiseres det at det ved vurderingen av egnet sikkerhetsnivå «særlig [skal] tas hensyn til risikoene forbundet med behandlingen, særlig som følge av utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet». Både i vurderingen av hvilke tiltak som må implementeres for å sikre tilstrekkelig internkontroll og i vurderingen av hvilke tiltak som i tilstrekkelig grad sikrer personopplysningene som behandles, står med andre ord risikovurderinger sentralt.

Videre kreves det etter artikkel 25 at det gjennomføres «egnede tekniske og organisatoriske tiltak […] utformet med sikte på en effektiv gjennomføring av prinsippene for vern av personopplysninger […] og for å integrere de nødvendige garantier i behandlingen for å oppfylle kravene i denne forordning og verne de registrertes rettigheter». Det innføres her en generell plikt til innebygd personvern, som innebærer at det fra begynnelsen av må utvikles løsninger og personverntiltak for behandling av personopplysninger.[98] Også dette kravets rekkevidde avhenger av den konkrete risikoen databehandlingen fører med seg, ved at det ved implementeringen av de egnede tekniske og organisatoriske tiltakene blant annet skal tas hensyn til «risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter som behandlingen medfører».[99]

Det nevnte kravet om informasjonssikkerhet i GDPR artikkel 32 gjelder både for behandlingsansvarlig og databehandler. Dersom virksomheten etter risikovurderingen som kreves her finner at databehandlingen sannsynligvis vil «medføre en høy risiko for fysiske personers rettigheter og friheter», skal det foretas en «vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet», jf. artikkel 35 nr. 1. I tilfeller der denne vurderingen tilsier at databehandlingen vil «medføre en høy risiko dersom den behandlingsansvarlige ikke treffer tiltak for å redusere risikoen», må den behandlingsansvarlige «rådføre seg med tilsynsmyndigheten», jf. artikkel 36 nr. 1.

Artikkel 35, sammenholdt med artikkel 32, gir dermed anvisning på omfattende krav til internkontroll, ved at behandlingsansvarlig og databehandler må foreta risikovurderinger tilknyttet enhver databehandling, med den hensikt å identifisere høyrisikosituasjoner. Sammenholdt med de øvrige bestemmelsene gjennomgått under dette punktet, blir det tydelig

[98] Wessel-Aas og Ødegaard (2018) s. 203.

at behandlingsansvarliges og databehandleres befatning med personopplysninger gjennomsyres av risikovurderinger.

Dette får også betydning for andre bestemmelser der det ikke er direkte henvist til risiko. For eksempel følger det av GDPR artikkel 28 at dersom den behandlingsansvarlige ønsker å ta i bruk en databehandler, må databehandleren som velges kunne gi «tilstrekkelige garantier» om gjennomføring av tiltak som er egnet til å sikre oppfyllelse av kravene i forordningen og som verner de registrertes rettigheter. I denne sammenheng er det relevant at involvering av en databehandler i seg selv utgjør en risiko. Dermed må vurderingen av om det gis «tilstrekkelige garantier» etter artikkel 28 sammenholdes med kravene i for eksempel artikkel 25 om innebygd personvern og artikkel 35 om vurdering av personvernkonsekvenser.[100] Med andre ord må behandlingsansvarlig vurdere risikoen ved å bruke den aktuelle databehandleren. Dette gjelder naturligvis også ved valg av databehandler fra utenfor EU/EØS.

Forordningens henvisning til risikovurderinger kan videre forstås i lys av at kravene som pålegges behandlingsansvarlige og databehandlere må samsvare med hva som er praktisk mulig. Den teknologiske utviklingen, samt kostnadene ved implementeringen av sikkerhetstiltakene, er derfor også relevante hensyn, jf. artikkel 25 nr. 1. Dersom en leser momentene i artikkel 24 og 25 i sammenheng, blir det derfor klart at det ikke kreves en implementering av tiltak som er umulig å gjennomføre, og heller ikke en implementering som er uproporsjonalt byrdefull.  I forlengelsen av det blir det tydelig at GDPR ikke stiller krav om at risikoen knyttet til behandling av personopplysninger er lik null.

Bestemmelsene i kapittel IV sier imidlertid ingenting eksplisitt om i hvilken grad tilsvarende risikovurderinger er relevante for kravene til overføringsgrunnlag i kapittel V om overføring av personopplysninger til tredjestater. Selv om behandlingsansvarlig må foreta risikovurderinger ved valg av databehandler, er det for eksempel ikke gitt at en lav sannsynlighet for myndighetsinnsyn kan gjøre overføringen lovlig, dersom tredjestatens lovgivning åpner for slikt innsyn på en måte som fra et europeisk perspektiv ikke er nødvendig i et demokratisk samfunn. I slike tilfeller er risikobildet et helt annet, ved at de

[100] Jarbekk mfl. (2019) s. 270-271.

registrertes rett til håndhevbare rettigheter og effektive rettsmidler står på spill. Implikasjonene av dette vil adresseres nærmere under punkt 3.5.

Den potensielle overføringsverdien fra den risikobaserte tilnærmingen som kommer til uttrykk i GDPR kapittel IV og til kapittel V kan imidlertid forstås på bakgrunn av tilnærmingens tette bånd til ansvarsprinsippet. Det tette båndet må igjen forstås i lys av personvernforordningen som en meta-regulering, hvilket vil være temaet i det følgende.

## 3.4 Den risikobaserte tilnærmingens bakgrunn – personvernforordningens tilblivelseshistorie og dens funksjon som meta-regulering

Meta-regulering[101] er betegnelsen på en type lovgivning der lovgiveren fastsetter en rekke regulatoriske mål, og overlater et større skjønn til de regulerte subjektene hva gjelder hvilke tiltak som er best egnet for å nå disse målene.[102] Dette er til forskjell fra såkalt command and control-regulering, som er en mer tradisjonell form for lovgivning. Da fastsetter lovgiver snarere forhåndsbestemte normer, som igjen er understøttet av sanksjoner.[103]

En særskilt utfordring med command and control-regulering er at det forutsetter at man fra myndighetshold i forkant vet best hva slags atferd som må kreves for å oppnå de regulatoriske målene.[104] Gellert fremhever at begge de to reguleringsmodellene baserer seg på proporsjonalitetstester – der man veier de regulatoriske målene opp mot kostnadene eller ulempene ved å oppnå dem – men med forskjellige utgangspunkt.[105] Mens man ved command and control-regulering foretar proporsjonalitetstesten *ex ante*, slik at resultatet av testen er det som nedfelles i loven, vil proporsjonalitetstesten ved meta-regulering foretas fra sak til sak og med hensyn til den konkrete konteksten. I denne sammenheng er det de regulerte subjektene som selv foretar balansetesten, og dermed avgjør hvilke tiltak som er best egnet for å oppnå

[101] Det brukes en rekke ulike betegnelser på de forskjellige reguleringsmodellene i litteraturen. I tillegg har modellene flere underkategorier. En mer detaljert gjennomgang av ulike kategorier og underkategorier av reguleringsmodellene foretas i Gellert (2020). For vårt formål – å forstå rasjonalet bak GDPR generelt og ansvarsprinsippet spesielt – er det imidlertid verken nødvendig eller hensiktsmessig å gå dypere inn i de ulike nyansene her, utover å sondere mellom meta-regulering og command and control som reguleringsmodeller.
[102] Gellert (2020) s. 19.
[103] Gellert (2020) s. 19.
[104] Gellert (2020) s. 89.
[105] Gellert (2020) s. 21.

de regulatoriske målene.[106] Her er det naturligvis relevant å ta hensyn til graden av risiko i den aktuelle saken, hvilket indikerer at meta-regulering og risikobasert tilnærming er to sider av samme sak.

GDPR bærer preg av å være en form for meta-regulering, noe som blir særlig tydelig i forordningens kapittel IV. Artikkel 24 og 25 i GDPR er typiske eksempler på bestemmelser i en slik lovgivningsmodell. Som det har fremgått under punkt 3.3, gir bestemmelsene anvisning på hvordan behandlingsansvarlige skal utøve sitt skjønn ved tolking og anvendelse av de øvrige reglene i GDPR.[107] På personvernområdet innebærer meta-regulering med andre ord at behandlingsansvarlige selv avgjør hvilke beskyttelsestiltak som er mest hensiktsmessige for å oppnå tilstrekkelig beskyttelse av personopplysningene i det konkrete tilfellet, ved å ta hensyn til alvorligheten i de potensielle skadene databehandlingen kan ha på datasubjektet, sammenholdt med sannsynligheten for slik skade.

Begrunnelsen for en slik reguleringsmodell blir tydelig dersom man ser nærmere på utfordringene ved modellens motstykke i command and control-regulering. I et personvernperspektiv innebærer sistnevnte modell at lovgiver må vite hvilke typer beskyttelsestiltak som egner seg best for å gi datasubjektene den ønskede beskyttelsen, *før* databehandlingen i det hele tatt er planlagt. I forlengelsen av dette oppstår problemet med det Ogus kaller «technical failures» i forbindelse med slik lovgivning, som sikter til den situasjonen der lovgiver har en utilstrekkelig ekspertise og innsikt til å kunne avgjøre hva som er de beste metodene for å nå de regulatoriske målene.[108] Dette må videre ses i sammenheng med den teknologiske utviklingen, som gjør det særlig vanskelig å utarbeide gode personvernregler *ex ante*. Kapasiteten når det kommer til innhenting, lagring og organisering av store mengder data har for det første økt betraktelig.[109] I tillegg har utviklingen i trådløs teknologi muliggjort overføring og lagring av data på tvers av landegrenser gjennom skytjenester, hvilket også ble adressert i reformprosessen frem mot GDPR som en utfordring som måtte håndteres.[110] Henvisningen til «den tekniske utviklingen» i forordningens artikkel 25 og 32 kan forstås i lys av dette.

[106] Gellert (2020) s. 21.
[107] Quelle (2017) s. 508-509.
[108] Ogus (2004) kapittel 55.
[109] Gellert (2020) s. 96.
[110] European Commission COM/2010/0609 s. 2.

Dertil kommer at det store spennet i ulike databehandlingssituasjoner gjør at man ved detaljregulering av databehandlingsvirksomhet gjerne får store og komplekse regelverk, som det er vanskelig å holde seg oppdatert på. Dette kan illustreres ved et eksempel fra rettstilstanden under personverndirektivet. Selv om heller ikke direktivet var en utpreget command and control-regulering, var de behandlingsansvarlige virksomhetene i enkelte land tillagt langt mindre fleksibilitet enn det som følger av GDPR. Ettersom EUs direktiver må implementeres av hver enkelt medlemsstat, som i denne sammenheng tillegges en viss skjønnsmargin hva gjelder utformingen av rettighetene og pliktene etter direktiver,[111] varierte det mellom medlemsstatene hvor stort ansvar og skjønn de behandlingsansvarlige fikk i forbindelse med databehandlingen. Frankrike var et av landene som ga de behandlingsansvarlige svært lite fleksibilitet, ved at det nasjonale datatilsynet ga detaljert veiledning for databehandlingen helt nede på saksnivå.[112] Den store og komplekse mengden med retningslinjer gjorde det svært utfordrende for virksomhetene å i det hele tatt skaffe oversikt over innholdet i egne plikter.[113] Videre ble det til og med observert at retningslinjene var så komplekse at behandlingsansvarlige bedrifter på forhånd visste at de ikke ville være i stand til å overholde samtlige av dem, hvilket resulterte i at de hadde egne budsjetter øremerket bøter fra datatilsynet.[114] Med en slik overregulering av behandlingsansvarliges virksomhet vil det med andre ord fort kunne oppstå brudd på regelverket, uavhengig av virksomhetenes gode tro.

Introduksjonen av ansvarsprinsippet og de tilhørende kravene om interne rutiner i GDPR kapittel IV, kom blant annet som en konsekvens av de nevnte utfordringene med ny teknologi og komplekse regelverk, og med et mål om å gjøre overholdelsen av personvernprinsippene mer effektiv for behandlingsansvarlige virksomheter.[115] Et viktig rasjonale bak meta-reguleringen er nemlig at det er subjektene for reguleringen – for GDPRs del først og fremst de behandlingsansvarlige – som står nærmest til å vurdere hvilke tiltak som er best egnet for å oppnå de regulatoriske målene, ved at de kjenner konteksten til den aktuelle databehandlingen.[116] Dette gir, ifølge Gellert, de aktuelle virksomhetene anledning til å «calibrate their obligations, and mobilise resources where it matters most»,[117] noe som også er

[111] Fredriksen og Mathisen (2014) s. 280.
[112] Gellert (2020) s. 99-100.
[113] Kuner (2008) s. 5.
[114] Bamberger og Mulligan (2013) s. 1600.
[115] European Commission SEC/2012/72 s. 43.
[116] Art 29 WP og Working Party of Police and Justice (2009) s. 79.
[117] Gellert (2020) s. 159.

fremhevet av Centre for Information Policy Leadership (heretter «CIPL»). CIPL er en global tenketank som i samråd med industriledere, reguleringsmyndigheter og politikere utvikler globale løsninger for å sikre best mulig praksis av personvern og forsvarlig bruk av data. CIPL publiserte i 2014 en rapport om ansvarsprinsippet og risikobasert tilnærming, der det ble fremhevet at poenget med en slik kalibrering av de behandlingsansvarliges plikter er å «avoid wasting scarce resources on less important or bureaucratic requirements that neither benefit individuals nor better protect their information».[118] GDPR som en meta-regulering, der behandlingsansvarlige og databehandlere tillegges en større plikt til å foreta risikovurderinger fra sak til sak, tillater med andre ord bedrifter som har befatning med personopplysninger å bruke sine ressurser på en hensiktsmessig måte.

Ved å tillegge behandlingsansvarlige virksomheter et større skjønn med hensyn til implementering av beskyttelsestiltak er med andre ord tanken at vedkommende virksomheter fordeler sine ressurser avhengig av hvor de trengs mest for å oppnå tilstrekkelig databeskyttelse, og at man på den måten oppnår en bedre og mer effektiv beskyttelse totalt sett. I reformprosessen frem mot GDPR fremhevet Artikkel 29-gruppen i denne sammenheng at «a data controller whose processing is relatively low risk may not have to do as much to comply with its legal obligations as a data controller whose processing is high risk».[119] På denne måten unngår man en såkalt «box-ticking»-praksis, der virksomheter krysser av på forhåndssatte databeskyttelsesvilkår, med det formål å være i overenstemmelse med forordningen snarere enn å sørge for adekvat beskyttelse.[120] Forordningen som meta-regulering gir med andre ord virksomheter et større spillerom når det kommer til å sikre tilstrekkelig personvern. Med større skjønn kommer imidlertid større ansvar, hvilket forklarer de mange kravene til internkontroll og dokumentasjon i GDPR kapittel IV, og som klarlegger sammenhengen mellom meta-regulering, risikobasert tilnærming og ansvarsprinsippet.

## 3.5 Hvilke krav stiller personvernforordningen kapittel V til beskyttelsestiltak ved overføring av personopplysninger til tredjestater?

[118] CIPL (2014) s. 12.
[119] A29WP Statement (2014) s. 2.
[120] Robinson mfl. (2009) del 9.

Bakgrunnen for at personvernforordningen inneholder et eget kapittel for overføringer til tredjestater er ifølge fortalepunkt 116 at slike overføringer kan medføre en større risiko for at de registrerte ikke har håndhevbare rettigheter, og et dårligere vern av personopplysninger.[121] Utgangspunktet etter artikkel 44 første punktum er derfor at overføringer til tredjestater ikke skal finne sted, med mindre det foreligger et særskilt overføringsgrunnlag. Mer konkret fremgår det av bestemmelsen at «[e]nhver overføring av personopplysninger som behandles eller skal behandles etter overføring til en tredjestat […] skal finne sted bare dersom den behandlingsansvarlige og databehandleren […] oppfyller vilkårene i [kapittel V]». I bestemmelsens andre setning presiseres det at bestemmelsene i dette kapittelet skal «sikre at det nivået for vern av fysiske personer som garanteres i denne forordning, ikke undergraves».

Vilkårene for å kunne overføre personopplysninger til tredjestater følger av forordningens artikkel 44-50. Fokuset i denne oppgaven er på overføringer på grunnlag av standard personvernbestemmelser vedtatt av Kommisjonen etter artikkel 46 nr. 2 bokstav c, jf. artikkel 46 nr. 1. Etter artikkel 46 nr. 1 kan nemlig behandlingsansvarlige eller databehandlere overføre personopplysninger til en tredjestat dersom de har «gitt nødvendige garantier, og under forutsetning av at de registrerte har håndhevbare rettigheter og effektive rettsmidler» (egen utheving). De standardiserte personvernbestemmelsene kan etter artikkel 46 nr. 2 bokstav c fungere som en slik nødvendig garanti.

Verken ordlyden i artikkel 46 eller de øvrige bestemmelsene i kapittel V nevner eksplisitt hva som mer bestemt skal til for at de standardiserte personvernbestemmelsene utgjør «nødvendige garantier» ved overføringer til tredjestater, eller hvorvidt risiko er relevant i denne vurderingen. Tilsvarende er det uklart ut fra ordlyden alene om vurderingen av om de registrerte har «håndhevbare rettigheter og effektive rettsmidler» skal ta utgangspunkt i en risikobasert eller en rettighetsbasert tilnærming.

Samtidig legger ordlyden «nødvendige garantier» – som i den engelske og offisielle versjonen er omtalt som «appropriate safeguards» – etter en naturlig språklig forståelse opp til en helhetlig vurdering av hvilke tiltak som er egnede til å sikre tilstrekkelig vern av de aktuelle personopplysningene. Sammenholdt med formålsbestemmelsen i artikkel 44, må vurderingen ta utgangspunkt i hva som er egnet til å sikre at beskyttelsesnivået etter GDPR ikke «undergraves», jf. bestemmelsens andre setning. Ordet «undergraves» indikerer på sin side at

[121] GDPR fortalepunkt 116.

beskyttelsesnivået ikke behøver å være identisk med det som gjelder etter GDPR. Dette bekreftes i Schrems II-dommen, der EU-domstolen presiserer at de nødvendige garantiene etter GDPR artikkel 46 skal sikre et beskyttelsesnivå som *i det vesentlige* tilsvarer det som gjelder i EU.[122]

For å avgjøre hva som skal til for at de standardiserte personvernbestemmelsene gir slike «nødvendige garantier» som kreves etter GDPR artikkel 46 nr. 1, og hvorvidt tilnærmingen til denne vurderingen er risikobasert, er det med andre ord nødvendig å se hen til det øvrige beskyttelsesnivået i GDPR. Det er i så måte relevant at personvernforordningen ikke krever et beskyttelsesnivå der risikoen for personvernbrudd er lik null, som vist under gjennomgangen av kapittel IV over. I forlengelsen av dette taler den gjennomgående tilstedeværelsen av risikobaserte bestemmelser i GDPR kapittel IV i seg selv for at en risikobasert tilnærming også er relevant etter kapittel V.

På den annen siden kan det hevdes at en grunnleggende forutsetning for bestemmelsene i kapittel IV er at myndighetene i landet personopplysningene befinner seg i er forpliktet til GDPR, og at det er dette som gjør det forsvarlig å overlate ansvaret for å foreta risikovurderinger til behandlingsansvarlig. Ved å holde personopplysningene innenfor EU/EØS, kan behandlingsansvarlige og databehandlere med andre ord legge til grunn at nasjonale myndigheter ikke vil pålegge dem plikter som er i strid med EU-retten. Denne forutsetningen slår naturligvis ikke til når personopplysningene er overført til et land som *ikke* er forpliktet til GDPR. I slike tilfeller står en derimot overfor en risikofaktor i form av myndigheter med potensielt uproporsjonalt inngripende overvåkningshjemler. Dette er en risikofaktor som kan være særlig vanskelig å håndtere for både små og store bedrifter, hvilket kan tilsi at det skjønnet som i lys av ansvarsprinsippet overlates til behandlingsansvarlig, i slike tilfeller må innsnevres betraktelig.

Den særskilte forutsetningen i artikkel 46 nr. 1 om at de registrerte må ha «håndhevbare rettigheter og effektive rettsmidler» ved overføring av personopplysninger til tredjestater kan forstås i lys av dette. Mens man for land som er forpliktet til GDPR kan presumere at borgerne har håndhevbare rettigheter og effektive rettsmidler, er dette rettigheter som står på spill når personopplysninger overføres ut av EU/EØS. Som nevnt innledningsvis under dette punkt, er foranledningen for de særskilte kravene i GDPR kapittel V nettopp den økte risikoen

[122] C-311/18 *Schrems II,* avsnitt 94. Se nærmere om dette under kapittel 5.2.

for krenkelse av fysiske personers rettigheter ved overføringer til tredjestater. Selv om gjennomgangen av GDPR kapittel IV viste at forordningen ikke krever at risikoen for personvernbrudd er lik null, kan det derfor argumenteres for en mer rettighetsbasert tilnærming i forbindelse med slike overføringer, ved at det stilles visse minstekrav til sikring av de registrertes håndhevbare rettigheter og effektive rettsmidler.

Samtidig behøver ikke den økte risikoen for krenkelse av fysiske personers rettigheter ved overføring av personopplysninger til tredjestater nødvendigvis å innebære at en risikobasert tilnærming ikke kan legges til grunn i slike tilfeller. Det kan vel så mye være *et moment* som det må tas særlig hensyn til i konsekvensdelen av nettopp en risikovurdering. I tillegg til arten av de aktuelle personopplysningene som overføres, herunder om de er særlig sensitive, vil et relevant moment i et slikt perspektiv for eksempel være hvorvidt mottakerstaten gir europeiske borgere effektive rettsmidler. Systemet og hensynene i GDPR kapittel V stenger med andre ord ikke for at den konkrete risikoen er relevant ved vurderingen av om et overføringsgrunnlag gir adekvat beskyttelse, og nærmere bestemt om de supplerende beskyttelsestiltakene er tilstrekkelige.

## 3.6 Sammenfatning

Det er etter dette klart at ordlyden i verken kapittel IV eller V i GDPR gir klare holdepunkter for en konklusjon i den ene eller andre retningen hva gjelder spørsmålet om den risikobaserte tilnærmingen gjør seg gjeldende ved overføring av personopplysninger til tredjestater. Kapittel IV gir grunnlag for et utgangspunkt om at risikoen ved vern av personopplysninger ikke må være eliminert, noe som kan tale for at samme betraktninger må gjøres gjeldende i relasjon til risikoen for innsyn fra mottakerstatens myndigheter ved overføring til tredjestater. Samtidig er forutsetningene ved slike overføringer helt annerledes, med den konsekvens at utgangspunktet fra kapittel IV ikke nødvendigvis kan overføres til kapittel V.

Derimot kan rasjonalet bak den risikobaserte tilnærmingen i kapittel IV muligens gi grunnlag for å trekke slutninger om tilnærmingens overføringsverdi til kapittel V. Risikovurderingene som bestemmelsene i kapittel IV gir anvisning på, må forstås i lys av ansvarsprinsippet i artikkel 5 nr. 2, som gjelder generelt for hele forordningen. Ansvarsprinsippet må igjen forstås som en sentral komponent i utformingen av personvernforordningen som en meta-regulering. Et viktig hensyn som ligger til grunn for denne utformingen er at behandlingsansvarlige skal

kunne kalibrere sine plikter og ressurser på en proporsjonal og skalerbar måte. Dette hensynet gjør seg også gjeldende ved overføring av personopplysninger til tredjestater, i den forstand at bedrifter eksempelvis kan allokere sine ressurser tilknyttet kostbare tekniske beskyttelsestiltak til situasjoner med middels til høy risiko for innsyn fra tredjestatens myndigheter. Motsetningsvis kan mindre kostbare tiltak iverksettes der det eksempelvis dreier seg om kontaktopplysninger som uansett er tilgjengelig på internett, og som nasjonale myndigheter formodentlig ikke vil kreve innsyn i. Personvernforordningens system, og hensynene bak dette, taler derfor for en risikobasert tilnærming ved vurderingen av hvilke beskyttelsestiltak som skal iverksettes ved overføring av personopplysninger til tredjestater.

Det var også en slik tilnærming Artikkel 29-gruppen virket å innta i sin veileder tilknyttet databehandling med høy risiko og tilhørende risikovurdering i artikkel 35.[123] I tilknytning til overføringer til tredjestater ble det fremhevet her at «transfers to third countries should not automatically and per se be seen as constituting high risk processing under GDPR. It should instead be determined whether such transfers could result in a high likelihood and severity of risk of harm, for example due to governmental access to that data».[124] Retningslinjene ble videreført av Personvernrådet 25. mai 2018.[125] Ettersom veilederen ble publisert i 2017 – tre år før Schrems II-dommen – har riktignok ikke Artikkel 29-gruppens uttalelser her nevneverdig vekt i forhold til nyere kilder som adresserer temaet. Likevel er uttalelsen egnet til å illustrere hvordan den risikobaserte tilnærmingen i GDPR også var tiltenkt overføringer til tredjestater.

Et gjennomgående tema i argumentasjonen rundt GDPR som meta-regulering er proporsjonalitet. I forlengelsen av dette er det relevant å løfte blikket til øvrig EU-rettslig lovgivning, herunder særlig EUs pakt om grunnleggende rettigheter, der proporsjonalitetsprinsippet fremheves i artikkel 52. I det følgende vil det foretas en vurdering av hvilken betydning dette kan ha for tolkningen av forordningen, særlig sett i lys av pakten artikkel 16 om friheten til å opprette og drive egen forretningsvirksomhet.

[123] A29WP Guidelines (2017).
[124] A29WP Guidelines (2017) s. 8.
[125] Oversikt over veiledere og retningslinjer fra Artikkel 29-gruppen som EDPB har gitt sin tilslutning til er tilgjengelig på https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en (sist lest 14.05.2021).

# 4 Hvilken betydning har Den europeiske unions pakt om grunnleggende rettigheter for spørsmålet om risiko ved overføringer til tredjestater?

## 4.1 Overordnet

Som nevnt under punkt 1.3, må tolkningen av EUs rettsakter foretas i tråd med sine hjemmelsgrunnlag. En sentral kilde som i denne sammenheng må tas hensyn til, er pakten. Etter artikkel 1 nr. 2 i GDPR skal forordningen «sikre […] vern av fysiske personers grunnleggende rettigheter og friheter, særlig deres rett til vern av personopplysninger». Ordlyden «grunnleggende rettigheter og friheter» peker hen på nettopp pakten, og det er «særlig» retten til vern av personopplysninger etter pakten artikkel 8 som gjennomføres og konkretiseres med GDPR.[126]

Selv om personopplysningsvernet er det som i første rekke skal ivaretas av GDPR, er det uunngåelig at ulike rettigheter og friheter tidvis vil kollidere. En viktig presisering i forlengelsen av dette fremgår av fortalepunkt 4 i forordningen, der det i andre setning presiseres at personopplysningsvernet ikke er en absolutt rettighet, og at den må veies mot andre grunnleggende rettigheter i samsvar med proporsjonalitetsprinsippet. Dette prinsippet legges også eksplisitt til grunn i pakten artikkel 52, som står sentralt ved tolkningen av de ulike rettighetene og frihetene som gjør seg gjeldende. I tråd med EU-rettslig metode må derfor GDPR tolkes på en slik måte at personopplysningsvernet avveies mot andre rettigheter og friheter på en proporsjonal måte, og etter forholdene bøyes av for disse.

Kollisjonen mellom personvernet og enkelte rettigheter og friheter er direkte adressert i GDPR, slik som i artikkel 85 om forholdet til ytrings- og informasjonsfriheten. For vår problemstilling er det imidlertid særlig friheten til å drive næringsvirksomhet som er av interesse. Den fremheves i fortalepunkt 4 som en frihet som ivaretas av GDPR, og følger av

[126] Skullerud mfl. (2018) s. 101.

artikkel 16 i EUs pakt om grunnleggende rettigheter. I det følgende vil det derfor redegjøres for forholdet mellom personvernet og friheten til å drive næringsvirksomhet.

## 4.2 Om friheten til å opprette og drive forretningsvirksomhet

Det følger av pakten artikkel 16 at «[t]he freedom to conduct a business in accordance with Union law and national laws […] is recognised». Friheten til å drive forretningsvirksomhet gjelder enhver fysisk og juridisk person, og omfatter enhver legitim form for profittskapende virksomhet.[127]

Ordlyden «is recognised» i artikkel 16 kan etter en naturlig språklig forståelse indikere en mer tilbakeholden beskyttelse enn det som gjelder for andre rettigheter og friheter. Formuleringen bærer preg av å være langt vagere enn det som gjelder ellers i pakten, som ellers stort sett viser til at «[e]veryone has the right to» den aktuelle rettigheten eller friheten, se eksempelvis artikkel 8 om personvern. Ordlyden kan dermed implisere at friheten til å drive forretningsvirksomhet ikke skal tillegges like stor vekt når den skal vurderes mot kolliderende rettigheter og friheter. Dette kan henge sammen med at økonomiske, sosiale og kulturelle rettigheter ofte bærer preg av å nettopp være vage og vanskelige å etterprøve for en domstol.[128]

Frihetens vage karakter kan imidlertid ikke gå på bekostning av proporsjonalitetsprinsippet i pakten artikkel 52, som uansett gjelder for alle anerkjente rettigheter og friheter. I bestemmelsens første setning fremheves det at enhver begrensning av de rettigheter og friheter som anerkjennes i pakten skal «respect the essence of those rights and freedoms». Ettersom det er begrenset med rettspraksis om pakten artikkel 16, herunder om intensjonsdybden i bestemmelsens formulering, er det ikke noe grunnlag for å fravike dette prinsippet.[129]

Som nevnt innledningsvis under punkt 1.2, er dagens økonomi i stor grad datadrevet, og overføring av personopplysninger på tvers av kontinenter er en viktig del av bedrifters daglige

[127] European Union Agency for Fundamental Rights (2015) s. 11.
[128] Nærmere om dette på Amnesty sine nettsider: https://amnesty.no/okonomiske-sosiale-og-kulturelle-rettigheter-retten-til-et-godt-liv-vart-nye-mal (sist lest 01.06.2021).
[129] Se Aall (2011) s. 31: «Selv om det kanskje er et trekk ved ØSK-rettighetene at deres rettskvalitet er ringere enn de sivile og politiske rettigheters, blir det for unyansert å hevde dette generelt».

virke. Kravet om supplerende beskyttelsestiltak ved overføring av personopplysninger til tredjestater utgjør dermed klart nok en begrensning i friheten til å drive forretningsvirksomhet i pakten artikkel 16. Vurderingen blir om det fordrer en risikobasert tilnærming til dette kravet for at det vesentligste innholdet i friheten respekteres, og hvorvidt begrensningen herfra av hensyn til personopplysningsvernet er proporsjonal, jf. pakten artikkel 52.

## 4.3 Betydning av proporsjonalitetsprinsippet og grunnrettighetspakten artikkel 16

Som det fremgikk under punkt 2.1, legger den risikobaserte tilnærmingen opp til en vurdering fra sak til sak av den konkrete risikoen som overføringen fører med seg, slik at risikonivået påvirker omfanget av tiltakene som må implementeres. Målet her er å *redusere* risikoen til et tilfredsstillende nivå. Motsetningsvis vil en mer rettighetsbasert tilnærming innebære et krav i retning av *eliminering* av risikoen for innsyn fra tredjestatens myndigheter, uavhengig av om denne risikoen er stor eller liten i utgangspunktet. Med andre ord dreier valget mellom en risikobasert eller en rettighetsbasert tilnærming seg om hvorvidt det er den *konkrete* risikoen eller den *teoretiske* risikoen som skal være utslagsgivende for kravet om supplerende beskyttelsestiltak.

Ettersom den rettighetsbaserte tilnærmingen i realiteten innebærer et krav om tekniske tiltak slik som sterk kryptering eller pseudonymisering,[130] vil denne tilnærmingen sette svært store begrensninger for europeiske bedrifters virksomhet. Majoriteten av overføringene som skjer ut fra Europa skjer i forbindelse med bedrifters bruk av skytjenester,[131] en type tjeneste som i sin natur ofte vil kreve tilgang til personopplysningene i sin «rene» form. Et praktisk eksempel er skybaserte e-posttjenester, som bistår med kommunikasjon ut til oppdragsgivers kunder, for eksempel i forbindelse med markedsføring.[132] For at en slik tjeneste i det hele tatt skal kunne gjennomføres, er databehandleren avhengig av å ha tilgang til de aktuelle kundenes e-postadresser.[133] Denne informasjonen kan derfor ikke pseudonymiseres, og den kan heller ikke være kryptert hele tiden under lagring. Et krav om at beskyttelsestiltakene fullt

[130] Jf. oppgavens punkt 2.1.
[131] Tene (2020).
[132] SendGrid er et eksempel på en amerikansk tilbyder av slik tjeneste, som på vegne av om lag 82,000 selskaper behandler to billioner e-postadresser (https://sendgrid.com/why-sendgrid/ (sist lest 04.04.2021)). Se nærmere om en av deres automatiserte e-posttjenester på https://sendgrid.com/solutions/email-marketing/automation/ (sist lest 04.04.2021).
[133] CIPL (2020), s. 14.

ut skal sikre de aktuelle personopplysningene mot innsyn fra tredjestatens myndigheter, innebærer dermed at et flertall av de overføringene som skjer til ulike tredjestater er ulovlige, og at bedrifter i lys av Schrems II-dommen må finne alternative tjenestetilbud fra EU-land eller land som er sertifisert etter GDPR artikkel 45.

For at en slik tilnærming til EU-domstolens krav om supplerende beskyttelsestiltak skal være i tråd med proporsjonalitetsprinsippet, forutsetter det at de lovlige alternativene er konkurransedyktige i forhold til tjenestene som tilbys i tredjestater. I motsatt fall vil resultatet være at bedrifter i stater som ikke er forpliktet til GDPR, får et stort konkurransefortrinn, ved å ha tilgang til et større og formodentlig mer kostnadseffektivt marked. I denne sammenheng er det relevant at en klar storpart av verdens teknologiselskaper er basert i USA eller Asia,[134] og at skytjenestetilbudet i Europa er dårligere i både omfang og kvalitet.[135] Det kan dermed argumenteres for at den rettighetsbaserte tilnærmingen setter europeiske bedrifter i en dårligere konkurransemessig posisjon globalt sett. Med andre ord innebærer en slik tilnærming potensielt store negative konsekvenser for disse bedriftene, hvilket trekker i retning av at den ikke sørger for en proporsjonal balansering av personvernet på den ene siden og friheten til å drive forretningsvirksomhet på den andre.

I tillegg kan det diskuteres hvorvidt en rettighetsbasert tilnærming til kravet om supplerende beskyttelsestiltak i det hele tatt er egnet til å gi personopplysningene *samlet sett* best mulig beskyttelse. Som vi har sett, kan denne tilnærmingen føre til en praksis hvor det stilles relativt like krav til ulike overføringer, uavhengig av risikonivået. Dersom man heller legger til grunn en risikobasert tilnærming ved overføring av personopplysninger til tredjestater, vil det gi bedriftene mulighet til å vurdere risikoen ved den aktuelle overføringen, og dermed hvilke tiltak som kreves i den konkrete saken. På denne måten kan bedriftene for eksempel allokere flere ressurser til implementering av omfattende beskyttelsestiltak ved mer risikable overføringer. Ved for eksempel å tillate kontraktsrettslige og organisatoriske tiltak, eller mindre omfattende krypteringsløsninger, ved overføring av lite sensitive personopplysninger som uansett er tilgjengelig på internett, er det bedre tilrettelagt for at bedriftene kan bruke sine ressurser på solid beskyttelse av mer risikable overføringer. Dette er i tråd med formålet bak den risikobaserte tilnærmingen slik det er presentert under punkt 3.4, der det fremgikk at den

[134] Nærmere om dette her: https://e24.no/boers-og-finans/i/m6bQOp/kommentar-hvor-er-europa-i-teknologikapploepet (sist lest 10.05.2021).
[135] Foss (2021) under kapittelet «Hva gjør leverandørene?».

risikobaserte tilnærmingen gir de behandlingsansvarlige anledning til å kalibrere sine plikter på en slik måte at deres ressurser først og fremst allokeres der de trengs mest, og at man dermed unngår å bruke begrensede ressurser på en unødvendig måte.

Den potensielle nytten ved gi behandlingsansvarlig muligheten til å kalibrere sine plikter i lys av den konkrete risikoen kan illustreres ved situasjonen for små og mellomstore bedrifter. For at paktens anerkjennelse av «freedom to conduct a business» etter artikkel 16 skal være reell, er det nødvendig å legge til rette for og muliggjøre skalerbar vekst for slike bedrifter. Med henvisning til at komplekse regler og administrative byrder ifølge disse bedriftene er en av de største hindringene for deltakelse i det økonomiske markedet, har Kommisjonen satt som mål å nettopp forenkle reglene og redusere disse byrdene for små og mellomstore bedrifter.[136] Strategien må forstås i lys av at slike bedrifter gjennomgående vil ha mindre ressurser en andre aktører i markedet, med den konsekvens at jo flere ressurser som må allokeres til administrative krav og formaliteter, desto vanskeligere er det å oppnå videre vekst. Det vil eksempelvis kunne bli tilfellet dersom en for stor andel av de begrensede ressursene til en nyoppstartet bedrift må brukes på implementering av krypteringsløsninger, eller etter forholdene dyrere tjenestetilbud fra Europa. Når store deler av små og mellomstore bedrifters økonomiske vekst kan tilskrives deres deltakelse i det globale markedet,[137] kan det derfor argumenteres for at et proporsjonalt inngrep i pakten artikkel 16 forutsetter at det tas utgangspunkt i den *konkrete* risikoen ved vurderingen av hvilke beskyttelsestiltak som skal implementeres.

Kommisjonens mål for små og mellomstore bedrifter er naturligvis ikke en rettskilde av nevneverdig vekt, men det illustrerer det reelle behovet for å tilrettelegge for disse bedriftenes videre vekst. Dersom kravene til beskyttelsestiltak er så strenge og udifferensierte at de står i veien for bedrifters vekst, vil det videre kunne resultere i at flere bedrifter heller tar sjansen på å overføre personopplysninger uten beskyttelsestiltak i det hele tatt, i håp om å ikke bli tatt.

Det kan også diskuteres i hvilken grad en rettighetsbasert tilnærming til kravet om supplerende beskyttelsestiltak i det hele tatt er egnet til å gi en bedre beskyttelse av de registrertes rettigheter, uavhengig av om kravet følges. Selv om de overførte personopplysningene er kryptert hele veien under lagring i den aktuelle tredjestaten, besitter

[136] European Commission COM/2020/103 s. 7.
[137] European Commission COM/2020/103 s. 11.

overvåkningsmyndighetene i stater som USA høyst sannsynlig nok teknisk kompetanse til å komme forbi slike tekniske tiltak.[138] Som påpekt av Christakis, kan et strengt krav om full kryptering eller pseudonymisering ved overføring til tredjestater dermed medføre at mottakerlandets overvåkningsmyndigheter tyr til enda mer inngripende måter å få tilgang til de aktuelle opplysningene.[139]

Ettersom en åpning for risikovurderinger på sin side utgjør et inngrep i personvernet og potensielt retten til effektive rettsmidler, må dette inngrepet naturligvis også være proporsjonalt. Dersom det skal overlates til dataeksportørene å foreta risikovurderinger for hver overføring, er det derfor verdt å minne om at grunnleggende rettigheter for den registrerte ligger i den andre vektskålen. De potensielle konsekvensene for de registrerte ved tilfeller av overvåkning fra tredjestatens myndigheter er derfor prinsipielt alvorlige, selv om de aktuelle opplysningene ikke er sensitive i seg selv. For at en overføring skal være i tråd med proporsjonalitetsprinsippet, må det derfor kunne påvises lav sannsynlighet for slikt innsyn.

Med dette forbeholdet legges det til grunn at pakten artikkel 16, sammenholdt med proporsjonalitetsprinsippet i artikkel 52, tilsier at bedrifter kan ha en risikobasert tilnærming til kravet om supplerende beskyttelsestiltak ved overføring av personopplysninger til tredjestater. Det vises særlig til at europeiske bedrifters muligheter for deltakelse i det globale markedet i motsatt fall vil begrenses betraktelig, og får konkurransemessige ulemper i forhold til bedrifter utenfor Europa. Dertil kommer at den risikobaserte tilnærmingen er egnet til å kalibrere bedriftenes plikter med hensyn til supplerende beskyttelsestiltak i forbindelse med overføringer til tredjestater – og dermed behovet for inngrep i friheten til å drive forretningsvirksomhet – med utgangspunkt i den konkrete risikoen for inngrep i øvrige rettigheter. En slik balansert rettstilstand er i kjernen av det proporsjonalitetsprinsippet er ment å føre med seg, og er videre egnet til å oppnå en best mulig beskyttelse av de registrertes personopplysninger samlet sett.

[138] Goodin (2015).
[139] Christakis (2020) del 2.

# 5 Schrems II

## 5.1 Overordnet

De foregående kapitlene i oppgaven har vist den tette sammenhengen mellom GDPR og EUs pakt om grunnleggende rettigheter. Denne sammenhengen er også fremtredende i Schrems II-dommen, der EU-domstolen gjennomgående presiserte at forordningens bestemmelser, herunder artikkel 46 om overføring på grunnlag av nødvendige garantier, må tolkes i lys av pakten. Særlig ble det vist til paktens bestemmelser i artiklene 7 og 8 om henholdsvis retten til respekt for privat- og familielivet og retten til personvern, og artikkel 47 om retten til effektive rettsmidler og en rettferdig rettergang.[140] Det er særlig disse rettighetene som står på spill når registrertes personopplysninger overføres til en tredjestat, noe som begrunner nødvendigheten av ytterligere beskyttelsestiltak.

I det følgende vil det foretas en nærmere gjennomgang av EU-domstolens syn på standardkontraktene som overføringsgrunnlag, herunder også begrunnelsen for kravet om supplerende beskyttelsestiltak punkt 5.2. Deretter vil dommens premisser tilknyttet dette kravet undergås en nærmere analyse i punkt 5.3, med sikte på å identifisere beveggrunner som kan si noe om hvorvidt domstolen åpner for en risikobasert tilnærming.

## 5.2 Nærmere om EU-domstolens tilnærming til standardkontraktene som overføringsgrunnlag

I vurderingen av EUs standardkontrakter som grunnlag for overføringer til tredjestater, tok EU-domstolen først stilling til hvilken grad av beskyttelse som i denne sammenheng må kreves, med henvisning til artikkel 46 nr. 1 og nr. 2 bokstav c. Domstolen la her til grunn at bestemmelsens henvisning til «nødvendige garantier» og «håndhevbare rettigheter og effektive rettsmidler» må forstås i lys av artikkel 44.[141] Av sistnevnte bestemmelse følger det at alle bestemmelsene i kapittel V i GDPR skal «sikre at det nivået for vern av fysiske personer som garanteres i denne forordning, ikke undergraves».

[140] Se for eksempel avsnitt 122 i dommen.
[141] C-311/18 *Schrems II,* avsnitt 92.

I forlengelsen av dette viste domstolen til at kravet om «tilstrekkelig beskyttelsesnivå» i artikkel 45 nr. 1, som regulerer overføringer på grunnlag av en adekvansbeslutning fra Kommisjonen, ikke innebærer et krav om at beskyttelsesnivået i tredjestaten er identisk med det som gjelder i EU, men at det må være *i det vesentlige* det samme.[142] Når en slik kommisjonsbeslutning derimot ikke foreligger, må derfor de «nødvendige garantie[ne]» etter artikkel 46 kompensere for den manglende databeskyttelsen i tredjestaten på en slik måte at en nettopp oppnår et beskyttelsesnivå som i det vesentlige tilsvarer det som gjelder i EU.[143] Når det kommer til sammenligningsgrunnlaget – *hva* beskyttelsesnivået i det vesentlige skal tilsvare – presiserte EU-domstolen at vurderingen må ta utgangspunkt i bestemmelsene i GDPR, lest i lys av EUs pakt om grunnleggende rettigheter.[144]

Videre vurderte domstolen hvorvidt Kommisjonens vedtakelse av de standardiserte personvernbestemmelsene er gyldig, hensett til pakten artikkel 7, 8 og 47.[145] De tre bestemmelsene gjelder henholdsvis retten til respekt for privat- og familieliv, retten til beskyttelse av personopplysninger og adgang til effektive rettsmidler og en upartisk domstol. Som utgangspunkt for denne vurderingen, fremhevet EU-domstolen det faktum at standardkontraktene kun er bindende for den behandlingsansvarlige parten fra EØS og mottakeren av personopplysningene i tredjestaten.[146] All den tid tredjestatens *myndigheter* ikke er part i avtalen, er de naturligvis ikke bundet av standardkontraktenes bestemmelser. Spørsmålet ble dermed om standardbestemmelsenes manglende evne til å gi beskyttelse mot myndighetene i den aktuelle tredjestaten, medfører at disse er ugyldige.[147]

EU-domstolen besvarte dette spørsmålet benektende.[148] På grunn av standardkontraktenes kontraktsrettslige natur, sammenholdt med artiklene 44, 46 nr. 1 og 46 nr. 2 bokstav c i GDPR, som tolket i lys av pakten krever at beskyttelsesnivået i forordningen ikke undergraves, kan det imidlertid være nødvendig å supplere personvernbestemmelsene med ytterligere beskyttelsestiltak.[149] Behandlingsansvarlig har med andre ord en plikt til å fra sak

[142] C-311/18 *Schrems II,* avsnitt 94.
[143] C-311/18 *Schrems II,* avsnitt 96.
[144] C-311/18 *Schrems II,* avsnitt 101.
[145] C-311/18 *Schrems II,* avsnitt 122.
[146] C-311/18 *Schrems II,* avsnitt 125.
[147] C-311/18 *Schrems II,* avsnitt 127.
[148] C-311/18 *Schrems II,* avsnitt 149.
[149] C-311/18 *Schrems II,* avsnitt 132.

til sak vurdere hvorvidt lovgivningen i tredjestaten gir tilstrekkelig beskyttelse, og der det er nødvendig implementere slike supplerende tiltak.[150]

Dette er i tråd med fortalepunkt 109 i GDPR, der det fremgår at muligheten for bruk av standardkontraktene «bør ikke hindre de behandlingsansvarlige eller databehandlere i å […] tilføye andre bestemmelser eller ytterligere garantier», og at behandlingsansvarlige og databehandlere tvert imot «bør oppmuntres til å fastsette ytterligere garantier gjennom avtalefestede forpliktelser som utfyller standard personvernbestemmelser». Dersom det derimot ikke lar seg gjøre å implementere supplerende tiltak som garanterer tilstrekkelig beskyttelse, må overføringen stanses.[151] Det vil etter EU-domstolens oppfatning for eksempel være tilfellet der lovgivningen i tredjestaten pålegger mottakeren av personopplysningene plikter som kolliderer med de standardiserte personvernbestemmelsene.[152] I slike tilfeller vil den aktuelle lovgivningen kunne stå i veien for de kontraktsrettslige garantiene som skal sikre tilstrekkelig beskyttelse mot innsyn fra tredjestatens myndigheter, og dermed risikere brudd på den registrertes rettigheter.

EU-domstolen sa imidlertid ingenting eksplisitt om *hva* de eventuelle supplerende beskyttelsestiltakene mer bestemt skal gå ut på. Det som er klart, er at det påhviler en plikt hos dataeksportøren til å foreta en konkret vurdering fra sak til sak om hvilke tiltak som er nødvendige for å oppnå et beskyttelsesnivå som i det vesentlige tilsvarer det som gjelder i EU. Domstolen sa heller ingenting eksplisitt om *hvordan* denne vurderingen skal foretas, og herunder hvilken rolle den konkrete risikoen skal spille. I det følgende skal det derfor foretas en nærmere analyse av dommen, med sikte på å identifisere uttalelser som kan trekke i retning av en rettighetsbasert eller risikobasert tilnærming til beskyttelsesnivået ved overføringer til tredjestater.

## 5.3 Åpner EU-domstolen for en risikobasert tilnærming ved overføring av personopplysninger til tredjestater?

EU-domstolen la tydelig til grunn at de standardiserte personvernbestemmelsene ikke alene gir tilstrekkelig beskyttelse der pliktene i disse bestemmelsene ikke respekteres av

[150] C-311/18 *Schrems II,* avsnitt 134.
[151] C-311/18 *Schrems II,* avsnitt 135.
[152] C-311/18 *Schrems II,* avsnitt 135.

tredjestatens lovgivning. Dette gjelder tilsynelatende uavhengig av sannsynligheten for at tredjestatens myndigheter ønsker innsyn i de aktuelle personopplysningene. I lys av dette kan det argumenteres for at EU-domstolen i Schrems II-dommen tok avstand fra den risikobaserte tilnærmingen ved overføring av personopplysninger til tredjestater.

Holdbarheten i en slik argumentasjon er imidlertid diskutabel. Dommen kan like fullt tolkes slik at domstolen simpelthen ikke anså en eventuell lav sannsynlighet for innsynsbegjæring fra myndighetshold som noe som kan veie opp for risikobildet totalt sett, dersom standardkontraktene utgjør den eneste beskyttelsen. Hensett til de potensielle konsekvensene som står på spill, som er at de registrertes grunnleggende rettigheter blir krenket, kan med andre ord risikoen her anses for å være for stor til at de standardiserte personvernbestemmelsene alene kan gi tilstrekkelig beskyttelse. Dette er imidlertid ikke det samme som et krav om *eliminering* av risiko. Domstolens konklusjon er med andre ord forenlig med en risikobasert tilnærming tilknyttet spørsmålet om hvilke tiltak som skal supplere disse bestemmelsene.

I tillegg kan domstolens uttalelser om de nasjonale datatilsynenes ansvar tolkes i retning av en risikobasert tilnærming til kravet om supplerende beskyttelsestiltak. Domstolen fremhevet at de europeiske datatilsynene skal avgjøre hvorvidt bedrifters bruk av de standardiserte personvernbestemmelsene er i tråd med GDPR.[153] Nærmere bestemt har datatilsynene, med henvisning til GDPR artikkel 58 nr. 2 bokstav f og j, en subsidiær plikt til å suspendere eller forby overføringer basert på personvernbestemmelsene dersom de finner at «in light of all the circumstances of that transfer, those clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer» (egen utheving).[154]

At det i vurderingen av om overføringen er i tråd med GDPR skal tas hensyn til *alle omstendighetene ved overføringen*, kan indikere at det skal foretas en helhetlig vurdering av risikobildet ved overføringen, før det avgjøres hvilke beskyttelsestiltak som er best egnet til å håndtere den aktuelle risikoen. Dette er vanskelig å forene med en mer rettighetsbasert tilnærming, der risikoen for innsyn fra myndighetshold må elimineres for at overføringen kan

[153] C-311/18 *Schrems II* avsnitt 146.
[154] C-311/18 *Schrems II* avsnitt 146.

finne sted. Med en slik tilnærming vil den eneste relevante omstendigheten ved vurderingen av beskyttelsesnivået i tredjestaten være om lovgivningen her i det hele tatt *åpner* for at myndighetene kan gi dataimportøren pålegg i strid med de standardiserte personvernbestemmelsene og EU-retten generelt. Det avgjørende her er som nevnt om det foreligger en teoretisk risiko for slike pålegg, og om det kan identifiseres beskyttelsestiltak som kan fjerne denne risikoen. Da ville det være unaturlig å tale om «all the circumstances of that transfer», som snarere legger opp til en mer skjønnsmessig vurdering.

Oppsummert gir ikke dommen klare svar på om den risikobaserte eller den rettighetsbaserte tilnærmingen skal legges til grunn for overføringer til tredjestater. Det som imidlertid er klart, er at den risikobaserte tilnærmingen ikke avvises i relasjon til overføring av personopplysninger til tredjestater. Dersom den konkrete risikoen ved overføringen er relevant for spørsmålet om hvilke supplerende beskyttelsestiltak som skal implementeres, legger riktignok EU-domstolen opp til en streng risikovurdering. Dersom lovgivningen i tredjestaten åpner for innsyn i europeiske borgeres personopplysninger på en – ut fra et EU-rettslig perspektiv – uproporsjonal måte, og dette kan gå på bekostning av forpliktelsene i de standardiserte personvernbestemmelsene som overføringen har grunnlag i, må ytterligere tiltak implementeres. Dette gjelder tilsynelatende uavhengig av sannsynligheten for at myndighetene kommer til å kreve innsyn i de aktuelle personopplysningene, og uavhengig av om disse opplysningene er helt enkle kontaktopplysninger som også er tilgjengelig andre steder. At de supplerende tiltakene må eliminere myndighetenes adgang til å gi slike pålegg, ga imidlertid ikke EU-domstolen holdepunkter for å legge til grunn.

I kjølvannet av dommen har Personvernrådet publisert en veileder som skal gi behandlingsansvarlige og databehandlere nærmere retningslinjer for hvordan kravene i Schrems II-dommen skal forstås.[155] Denne vil det gjøres nærmere rede for under neste punkt. EU-kommisjonen har i tillegg publisert et forslag til nye standardiserte personvernbestemmelser som skal gjelde ved overføringer til tredjestater.[156] Her gis det uttrykk for en alternativ forståelse av dommens krav enn den Personvernrådet legger til grunn, hvilket vil forklares nærmere under punkt 7.1.

[155] EDPB Recommmendations 01/2020.
[156] Draft implementing decision (2020).

# 6 Veileder fra Personvernrådet

## 6.1 Overordnet om veilederens innhold

I veilederen gir Personvernrådet anvisning på en seksstegs vurdering som må foretas ved overføring av personopplysninger til tredjestater.[157] For det første (1) må dataeksportøren skaffe oversikt over alle eventuelle overføringsaktiviteter til tredjestater. Dernest (2) må det undersøkes hvilket overføringsgrunnlag som tas i bruk for hver enkelt overføring. Det må her tas utgangspunkt i de alternative grunnlagene i GDPR kapittel V. Dersom Kommisjonen i medhold av artikkel 45 har fattet en beslutning om tilstrekkelig beskyttelsesnivå for den aktuelle mottakerstaten, eller dersom overføringen skjer på grunnlag av den snevre unntaksadgangen i artikkel 49, er overføringen lovlig.

Ved bruk av «nødvendige garantier» i medhold av artikkel 46, slik som standard personvernbestemmelser etter artikkel 46 nr. 2 bokstav c, må eksportøren bevege seg videre til neste steg. Dette steget går ut på (3) å vurdere mottakerlandets beskyttelsesnivå, i hovedsak basert på relevant nasjonal lovgivning tilknyttet den aktuelle overføringen.[158] Dersom man i denne vurderingen finner at beskyttelsesnivået ikke i det vesentlige tilsvarer det som gjelder i EU, må det (4) vurderes om det kan iverksettes supplerende beskyttelsestiltak som kompenserer for dette. For de tilfeller der slike tiltak kan identifiseres, gir veilederen anvisning på (5) hvordan selve implementeringen av tiltakene skal foregå. Her presiseres det blant annet at dersom overføringen skjer med grunnlag i standardkontraktene, og dette suppleres blant annet med ytterligere kontraktsvilkår, må det påses at de supplerende vilkårene ikke kolliderer med de standardiserte personvernbestemmelsene.[159] Til slutt må det foretas (6) fortløpende vurderinger av om overføringsgrunnlaget og de supplerende tiltakene gir tilstrekkelig beskyttelse.

For oppgavens problemstilling er det særlig steg 3 og 4 som er av interesse, da disse sier noe om de vurderingene behandlingsansvarlig må ta i forbindelse med overføringer til tredjestater,

[157] EDPB Recommendations 01/2020 s. 2.
[158] EDPB Recommendations 01/2020 s. 3.
[159] EDPB Recommendations 01/2020 s. 17.

herunder også om adgangen til å vurdere risiko. Dette vil det gjøres nærmere rede for i det følgende.

## 6.2 Veilederens tilnærming til risiko

I vurderingen under steg 3 er det først relevant å identifisere hvilken type overføring det dreier seg om, for å avgjøre hvilken del av den nasjonale lovgivningen som kommer til anvendelse.[160] Dernest må det tas stilling til om den aktuelle nasjonale lovgivningen i mottakerlandet svekker effekten av det overføringsgrunnlaget overføringen baserer seg på.[161] Her vil det være særlig viktig å undersøke de delene av nasjonal lovgivning som gir myndighetene adgang til å pålegge utlevering av personopplysninger, typisk av hensyn til nasjonal sikkerhet.[162] For at et slikt pålegg skal være lovlig i et EU-rettslig perspektiv, må myndighetenes innsynsadgang være «et nødvendig og forholdsmessig tiltak i et demokratisk samfunn» for å sikre et legitimt formål, slik det fremgår av artikkel 23 nr. 1 i GDPR.

For de tilfeller der relevant nasjonal lovgivning ikke er tilgjengelig – hvilket ofte er tilfellet for nasjonal overvåkningslovgivning[163] – skal det ses hen til andre *objektive* faktorer.[164] Eksempler på slike faktorer er blant annet resolusjoner og rapporter fra mellomstatlige organisasjoner og rapporter fra akademiske institusjoner og bransjeorganisasjoner.[165]

Særlig interessant for oppgavens problemstilling er at Personvernrådet deretter legger eksplisitt til grunn at man i vurderingen av beskyttelsesnivået ikke kan ta hensyn til subjektive faktorer slik som *sannsynligheten* for at tredjestatens myndigheter ønsker tilgang til de aktuelle personopplysningene.[166] Som nevnt under punkt 2.1, er sannsynligheten for inngrep i datasubjektenes rettigheter et sentralt element i den risikobaserte tilnærmingen. Med en slik tilnærming ville det vært naturlig å fastsette risikoen ved den aktuelle overføringen, for så å identifisere supplerende tiltak som kan senke risikoen til et tilfredsstillende nivå.

Etter Personvernrådets oppfatning skal man derimot identifisere om det i det hele tatt er en *mulighet* for at tredjestatens myndigheter kan gi mottakeren av personopplysningene pålegg

[160] EDPB Recommendations 01/2020 s. 12, avsnitt 32.
[161] EDPB Recommendations 01/2020 s. 13, avsnitt 34.
[162] EDPB Recommendations 01/2020 s. 13, avsnitt 36.
[163] Rubinstein og Margulies (2021) s. 23.
[164] EDPB Recommendations 01/2020 s. 14, avsnitt 42.
[165] EDPB Recommendations 01/2020 s. 38, avsnitt 138.
[166] EDPB Recommendations 01/2020 s. 14, avsnitt 42.

som strider mot de standard personvernbestemmelsene, og så om det finnes tiltak som eliminerer denne muligheten. Dette blir tydelig i veilederens eksemplifisering med utgangspunkt i amerikansk overvåkningslovgivning. Dersom dataimportøren faller inn under anvendelsesområdet til FISA 702, kan overføringsgrunnlaget kun anvendes dersom det implementeres supplerende, tekniske tiltak som gjør tilgangen til opplysningene «impossible or ineffective».[167] I forlengelsen av dette fremheves det under steg 4 i veilederen at supplerende beskyttelsestiltak kan være tekniske, kontraktuelle og organisatoriske,[168] men at det i realiteten alltid vil være nødvendig med tekniske tiltak slik som kryptering, ettersom det kun er slike tiltak som fullt ut forhindrer tredjestatens myndigheter fra å få tilgang til de aktuelle opplysningene.[169] Med andre ord kan det synes som at Personvernrådet i denne sammenheng inntar en rettighetsbasert tilnærming, slik denne er definert over under punkt 2.1.

Dette blir særlig tydelig i vedlegg 2 til Personvernrådets veileder, der Rådet presenterer syv eksempeltilfeller («Use Cases»), med konkretiseringer av hvordan kravet til supplerende beskyttelsestiltak gjør seg gjeldende i de ulike tilfellene.[170] Særlig er det sjette eksempeltilfellet («Use Case 6») egnet til å illustrere Personvernrådets rettighetsbaserte tilnærming ved overføring av personopplysninger til tredjestater. Eksempeltilfellet gjelder overføringer til skytjenesteleverandører eller andre databehandlere som krever tilgang til ukrypterte personopplysninger – «data in the clear» – for å kunne yte den aktuelle tjenesten.[171] I slike tilfeller viser Personvernrådet til at dersom tredjestatens lovgivning gir sine myndigheter videre innsynsfullmakter enn det som er nødvendig og proporsjonalt i et demokratisk samfunn, er det ingen beskyttelsestiltak som effektivt kan motvirke innsyn.[172] Konsekvensene av dette er, ifølge Rådet, at det for slike databehandlertjenester ikke er mulig å identifisere noen supplerende beskyttelsestiltak som kan sikre et adekvat beskyttelsesnivå.[173]

Personvernrådets presisering om at sannsynligheten for innsynsbegjæring ikke er relevant, kan vise seg å være problematisk i lys av EU-domstolens krav om at overføring av

[167] EDPB Recommendations 01/2020 s. 15, avsnitt 44.
[168] EDPB Recommendations 01/2020 s. 15, avsnitt 47.
[169] EDPB Recommendations 01/2020 s. 14, avsnitt 48.
[170] EDPB Recommendations 01/2020 s. 22 flg.
[171] EDPB Recommendations 01/2020 s. 26-27, avsnitt 88-89.
[172] EDPB Recommendations 01/2020 s. 27, avsnitt 88.
[173] EDPB Recommendations 01/2020 s. 27, avsnitt 89.

personopplysninger til tredjestater kun kan skje dersom et adekvat beskyttelsesnivå er sikret. En slik tilnærming innebærer i praksis et absolutt forbud mot bruk av en rekke skytjenester fra land der beskyttelsesnivået ikke i det vesentlige tilsvarer det europeiske, slik som fra USA. Ut fra det som har fremgått under punkt 4.3 om utbredelsen av slike skytjenester på verdensbasis, er det med andre ord i praksis tale om et forbud mot majoriteten av de skytjenestene som eksisterer på markedet.

Samtidig kan deler av Personvernrådets omtale av steg 4 indikere en slags risikobasert tilnærming. Ved avgjørelsen av hvilke beskyttelsestiltak overføringsgrunnlaget skal suppleres med, skal det tas hensyn til momenter som arten av personopplysningene, overføringens varighet og kompleksitet, mulighetene for at mottakeren vil overføre opplysningene videre til underleverandører og formatet personopplysningene overføres i, herunder om de er pseudonymisert eller kryptert.[174] Personvernrådet utdyper ikke hvilken betydning de ulike momentene vil ha ved identifiseringen av egnede beskyttelsestiltak, men flere av momentene står sentralt ved vurdering av risiko. For tilfeller der alvorlighetsgraden ved en databehandling skal vurderes, vil for eksempel arten av opplysningene være relevant. Dersom det dreier seg om sensitive personopplysninger som nevnes i artikkel 9 nr. 1 i GDPR, vil det trekke i retning av at databehandlingen innebærer en stor risiko, som igjen krever sterke beskyttelsestiltak.

Hvis det derimot dreier seg om lite private eller sensitive personopplysninger, som man gjerne også finner åpent tilgjengelig på internett, vil det på sin side tale for en lav risiko. Tilsvarende vil overføringens varighet og kompleksitet, samt mulighetene for videre overføringer til underleverandører, kunne si noe om sannsynligheten for inngrep i datasubjektenes rettigheter. Ved en enkel og kortvarig overføring, der kun et fåtall får tilgang til opplysningene, vil sannsynligheten være mindre for at de aktuelle personopplysningene kommer på avveie.

Veilederen fra Personvernrådet er med dette ikke helt konsekvent. Dersom en skal ta hensyn til samtlige av disse momentene ved identifiseringen av de egnede beskyttelsestiltakene ved en konkret overføring, vil det være lite forenlig med Personvernrådets uttalelse om at beskyttelsestiltakene skal gjøre tilgangen til de overførte personopplysningene «impossible or ineffective» for tredjestatens myndigheter. Forutsetningen for at man i det hele tatt befinner seg på steg 4, er at man på steg 3 fant at beskyttelsesnivået i mottakerlandet ikke er tilstrekkelig. Da vil det i realiteten bare være personopplysningenes *format* – om de er

[174] EDPB Recommendations 01/2020 s. 16, avsnitt 49.

kryptert eller pseudonymisert – som er av relevans dersom sistnevnte krav legges til grunn. Denne inkonsekvensen kan tilsi at behandlingsansvarlige og databehandlere bør unngå å legge Personvernrådets uttalelser ukritisk til grunn når de skal skaffe oversikt over sine plikter ved overføring av personopplysninger til tredjestater.

## 6.3 Hvordan er veilederen fulgt opp på nasjonalt nivå i EU/EØS?

Det er fortsatt begrenset med saker på nasjonalt nivå der Schrems II-dommen er adressert. I skrivende stund har det bayerske og det portugisiske datatilsynet fattet hver sin avgjørelse som tar for seg denne problematikken. I tillegg har den franske forvaltningsdomstolen Conseil d'État avsagt en kjennelse der Schrems II-dommens krav om supplerende beskyttelsestiltak adresseres. Selv om verken nasjonal tilsynspraksis eller praksis fra den franske forvaltningsdomstolen er rettskilder av nevneverdig vekt, er det for oppgavens del interessant å identifisere hvorvidt Personvernrådets rettighetsbaserte tilnærming er fulgt opp i praksis.

*Det bayerske datatilsynet*[175] erklærte den 15. mars 2021 at et tysk selskaps overføring av personopplysninger til USA i forbindelse med bruk av e-posttjenesten Mailchimp var ulovlig.[176] Ifølge datatilsynet var det indikasjoner på at Mailchimp var underlagt amerikansk overvåkningslovgivning (FISA 702) og at e-postadressene derfor sto i fare for å bli tilgjengeliggjort for amerikanske etterretningstjenester. Overføringen baserte seg på EUs standardiserte personvernbestemmelser, men selskapet hadde ikke vurdert potensielle supplerende beskyttelsestiltak for å sikre opplysningene mot amerikanske myndigheter. I lys av kravene etter Schrems II-dommen kom tilsynet derfor til at overføringen var ulovlig etter GDPR kapittel V, og at overføringen måtte opphøre.

Det bayerske datatilsynet tok ikke nærmere stilling til den konkrete risikoen ved overføringene, og viste heller ikke til Personvernrådets veileder. At det ikke ble foretatt en vurdering av blant annet sannsynligheten for myndighetsinnsyn i strid med EU-retten er naturlig, ettersom behandlingsansvarlig ikke hadde vurdert behovet for supplerende tiltak i det

[175] https://www.lda.bayern.de/de/index.html (sist lest 28.05.2021).
[176] https://edpb.europa.eu/news/national-news/2021/bavarian-dpa-baylda-calls-german-company-cease-use-mailchimp-tool_en (sist lest 28.05.2021).

hele tatt. Dermed ble ikke spørsmålet om en risikobasert tilnærming satt på spissen, ettersom kravene etter Schrems II-dommen uansett ikke var oppfylt.

*Det portugisiske datatilsynet*[177] beordret den 28. april 2021 det nasjonale instituttet for statistikk (Instituto Nacional de Estatística) om å stanse all overføring av personopplysninger til den USA-baserte tjenesten Cloudflare.[178] I forbindelse med en folketelling hadde instituttet samlet inn opplysninger om seks millioner portugisiske innbyggere. Tellingen innebar blant annet innsamling av helseopplysninger og opplysninger om innbyggernes trosoppfatning. Med andre ord dreide det seg om slike personopplysninger som fremheves som særlig sensitive i GDPR artikkel 9. Ved å bruke nettverkstjenesten Cloudflare overførte instituttet disse opplysningene til en rekke tredjestater, slik som USA, Kina, India og Russland.

Tilsynet viste blant annet til at instituttet i denne sammenheng kun hadde foretatt en utredning av konsekvensene ved statistikkinnhenting generelt, og ikke en vurdering av konsekvensene ved de aktuelle databehandlingsaktivitetene. Dermed ble det ikke lagt opp til en konkret vurdering av risikoen ved å overføre de innhentede personopplysninger ut av EU/EØS. Ytterligere tiltak kunne etter datatilsynets oppfatning minsket risikoen for personvernbrudd. Opplysningene var riktignok kryptert, men det var kun Cloudfare som satt på krypteringsnøkkelen. I forlengelsen av dette presiserte tilsynet at EUs standardiserte personvernbestemmelser ikke gir tilstrekkelig beskyttelse i seg selv, og at det i lys av Schrems II-dommen og ansvarsprinsippet i artikkel 5 nr. 2 må implementeres supplerende beskyttelsestiltak. Behovet for slike tiltak var ikke vurdert fra instituttets side, med den konsekvens at overføringene måtte opphøre.

Heller ikke i denne saken ble Personvernrådets tilnærming satt på spissen. All den tid det dreide seg om overføring av sensitive personopplysninger, uten at noen som helst vurdering av behovet for supplerende tiltak for den nevnte overføringen ble foretatt, var det klart nok tale om et brudd på kravene etter Schrems II-dommen.

Felles for de to nevnte sakene er at behandlingsansvarlig ikke hadde foretatt noen forhåndsvurdering av det konkrete behovet for supplerende tiltak i det hele tatt, hvilket ble særskilt fremhevet av de respektive datatilsynene. Selv om tilsynene ikke hadde noen

[177] https://www.cnpd.pt/ (sist lest 24.05.2021).
[178] https://edpb.europa.eu/news/national-news/2021/census-2021-portuguese-dpa-cnpd-suspended-data-flows-usa_en?s=09 (sist lest 24.05.2021).

foranledning til å ta stilling til om sannsynligheten for myndighetsinnsyn i strid med EU-retten er en relevant faktor, kan det derfor stilles spørsmål ved om resultatet hadde vært annerledes dersom behandlingsansvarlig hadde kunnet dokumentere en forutgående risikovurdering, med tilhørende tiltak avpasset etter den konkrete risikoen. I denne sammenheng kan det presiseres at dersom datatilsynene hadde lagt Personvernrådets tilnærming til grunn, ville det uansett ikke vært nevneverdig mye rom for en konkret vurdering av behovet for beskyttelsestiltak, utover å identifisere hvorvidt mottakerstatenes lovgivning åpner for myndighetsinnsyn i strid med EU-retten. Da ville det vært naturlig å adressere dette, samt hvilke tiltak som er egnet til å beskytte mot denne risikoen.

Videre avsa *Conseil d'État* den 12. mars 2021 kjennelse i en sak mellom det franske helsedirektoratet og Interhop med flere.[179] Helsedirektoratet hadde engasjert Doctolib, som spesialiserer seg i bookingtjenester på nett for helsevirksomheter, til å opprette en plattform for bestilling av Covid-19-vaksinasjon.[180] Doctolib brukte i denne sammenheng Luxembourg-baserte AWS Sarl som skytjenesteleverandør, som er datterselskap til det amerikanske selskapet Amazon Web Services. Selv om AWS Sarl sin behandling av de aktuelle personopplysningene ikke innebar at opplysningene ble overført ut av EU/EØS, kom Conseil d'État til at kravet om supplerende beskyttelsestiltak etter Schrems II-dommen gjorde seg gjeldende. Det ble i denne sammenheng vist til at databehandlerens morselskap var underlagt amerikansk lovgivning, og at det derfor forelå en risiko for innsyn fra amerikanske myndigheter etter FISA 702 og EO 12333.

Domstolen konkluderte imidlertid med at kravene etter GDPR og Schrems II-dommen var oppfylt, blant annet med henvisning til at personopplysningene var kryptert, og at det var en sertifisert tredjepart som satt på krypteringsnøkkelen. Heller ikke her kom den risikobaserte tilnærmingen på spissen, all den tid beskyttelsestiltakene som var implementert uansett gjorde det umulig for databehandleren å utlevere de aktuelle personopplysningene til amerikanske overvåkningsmyndigheter. Tiltakene ga med andre ord tilstrekkelig beskyttelse, uavhengig av om det er den risikobaserte eller den rettighetsbaserte tilnærmingen som legges til grunn.

[179] Kjennelsen kan lastes ned på https://www.conseil-etat.fr/en/news/the-urgent-applications-judge-does-not-suspend-the-partnership-between-the-ministry-of-health-and-doctolib-for-the-management-of-covid-19-vaccinati (på fransk).
[180] https://iapp.org/news/a/why-this-french-court-decision-has-far-reaching-consequences-for-many-businesses/ (sist lest 27.03.2021).

Conseil d'État uttalte ingenting om hvorvidt beskyttelsestiltakene som var implementert var nødvendige for at den aktuelle databehandlingen kunne anses som lovlig, eller om også mindre omfattende tiltak kunne tilfredsstilt kravene etter GDPR og Schrems II-dommen. Dersom domstolen hadde lagt til grunn Personvernrådets tilnærming, og dermed ment at de beskyttelsestiltak som var implementert måtte være et minstekrav – uavhengig av sannsynligheten for myndighetsinnsyn – ville det imidlertid vært naturlig å adressere. Det kan i denne sammenheng vises til at den krypteringsløsningen som ble brukt, der verken AWS Sarl i Luxembourg eller AWS i USA hadde tilgang til krypteringsnøkkelen, er et skoleeksempel på hvordan Personvernrådets veileder kan følges i praksis.

Det skal imidlertid ikke legges for mye i den manglende henvisningen til veilederen i de tre sakene. Ettersom det kun dreide seg om en *kjennelse* fra Conseil d'État, er det naturlig at det ikke ble foretatt noen uttømmende gjennomgang av rettskildebildet tilknyttet Schrems II-dommens krav om supplerende beskyttelsestiltak. I tillegg var det ikke tale om en overføring ut av EU/EØS. Selv om domstolen anerkjente at det forelå en risiko for at amerikanske myndigheter kunne få tilgang til de aktuelle personopplysningene, er det derfor uklart om den ville lagt til grunn andre krav i en tenkt sak der det rent faktisk hadde funnet sted en overføring til en tredjestat.

Dertil kommer at de faktiske forholdene i alle de tre sakene var av en slik karakter at kravene etter Schrems II-dommen klart kunne legges til grunn som oppfylt eller ikke. Med andre ord var ikke valget mellom en risikobasert tilnærming og Personvernrådets rettighetsbaserte tilnærming avgjørende for resultatet i disse sakene. Det fører derfor lite med seg å spekulere i hvordan de ulike organene hadde konkludert under andre omstendigheter, og hvorvidt de da ville tatt hensyn til sannsynligheten for myndighetsinnsyn i strid med EU-retten.

Uansett er det interessant at en så sentral kilde for forståelsen av Schrems II-dommens krav om supplerende beskyttelsestiltak ikke nevnes i det hele tatt. Det kan illustrere den usikre rettstilstanden både Schrems II-dommen og Personvernrådets veileder har etterlatt seg, og at veilederen ikke er tilstrekkelig overbevisende til at nasjonale organer tar den aktivt i bruk i sin rettsanvendelse.

# 7 Kommisjonens forslag til nye standardiserte personvernbestemmelser

## 7.1 Overordnet om Kommisjonens forslag

Dagen etter Personvernrådets publisering av veilederen om supplerende beskyttelsestiltak, publiserte EU-kommisjonen et forslag til nye standardiserte personvernbestemmelser.[181] Disse er ment å være bedre tilpasset kravene etter Schrems II-dommen, og skal erstatte personvernbestemmelsene Kommisjonen vedtok i 2001/2004[182] og 2010[183]. Forslaget var ute på høring frem til 21. desember 2020, mens det endelige vedtaket ble fattet av Kommisjonen 4. juni 2021.[184]

I forhold til de gjeldende personvernbestemmelsene vedtatt av Kommisjonen i medhold av artikkel 46 nr. 2 i forordningen, er nyvinninger i Kommisjonens forslag blant annet at det dekker flere partskonstellasjoner,[185] og at det oppfyller kravene til databehandleravtaler etter personvernforordningen artikkel 28 nr. 3. Det er dermed ikke lenger nødvendig med en slik avtale *i tillegg til* de standardiserte personvernbestemmelsene. Særlig interessant for vårt formål er imidlertid de skjerpede kravene til varsling om lokal lovgiving som strider mot EU-retten. I det følgende vil det vurderes hvorvidt Kommisjonens uttalelser tilknyttet dette kravet kan anses for å gi uttrykk for en risikobasert tilnærming.

## 7.2 Gir Kommisjonens forslag anvisning på en risikobasert tilnærming ved overføring av personopplysninger til tredjestater?

[181] Draft implementing decision (2020).
[182] Decision 2001/497/EC og Decision 2004/915/EC.
[183] Decision 2010/87/EU.
[184] Som nevnt under punkt 1.3, fotnote 62, tar oppgavens analyse kun utgangspunkt i Kommisjonens utkast, og ikke det endelige vedtaket. De poenger som gjøres gjeldende under punkt 7.2 er imidlertid fortsatt relevante etter Kommisjonens vedtak av 4. juni 2021 (se fotnote 190 i denne oppgaven).
[185] De nåværende standardiserte personvernbestemmelsene er kun tilrettelagt for overføringer fra behandlingsansvarlige til behandlingsansvarlige eller databehandlere, mens Kommisjonens forslag også dekker partskonsellasjonene der overføringen skjer fra databehandler til behandlingsansvarlig eller fra databehandler til databehandler. Se Foss (2021) for nærmere gjennomgang av endringene.

Som en konsekvens av Schrems II-dommen er det i klausul 2 i Kommisjonens forslag del II inntatt en rekke bestemmelser som adresserer problematikken rundt myndighetsinnsyn ved overføring av personopplysninger til tredjestater.[186] I henhold til klausul 2 bokstav a må partene erklære at de ikke har «reason to believe» at tredjestatens lovgivning forhindrer dataimportøren i å etterleve forpliktelsene i de standardiserte personvernbestemmelsene, herunder i form av krav om å utlevere personopplysninger til myndighetene. Klausul 2 bokstav b punkt (i) presiserer hva partene i denne sammenheng skal ta i betrakting. Her vises det blant annet til «any relevant practical experience with prior instances, or the absence of requests for disclosure from public authorities received by the data importer for the type of data transferred» som en relevant faktor (egen understreking).

At bestemmelsen legger opp til en vurdering av de praktiske erfaringene med innsynsbegjæringer fra tredjestatens myndigheter, indikerer at Kommisjonen anser den konkrete *sannsynligheten* for innsyn som relevant for partenes vurdering av om de har «reason to believe» at tredjestatens lovgivning står i veien for overholdelse av de standardiserte personvernbestemmelsene, jf. forslagets del II, klausul 2 bokstav a. Dersom sannsynlighetsbetraktninger *ikke* skulle vært relevant, ville det ikke vært behov for å ta hensyn til slike praktiske erfaringer, all den tid den eneste relevante faktoren i så fall vil være hvorvidt rettstilstanden i tredjestaten *åpner* for det som etter EU-retten vil være uproporsjonale inngrep i personvernet. Implikasjonene av en slik tolkning er at vurderingen av om de supplerende beskyttelsestiltakene som kreves etter Schrems II-dommen er egnet til å sikre et tilstrekkelig beskyttelsesnivå, vil variere med den konkrete risikoen i saken. Kommisjonen kan med andre ord hevdes å innta en risikobasert tilnærming til EU-domstolens krav ved overføring av personopplysninger til tredjestater, i strid med Personvernrådets veiledende uttalelser.

At Kommisjonen har en annen tilnærming enn Personvernrådet kommer også klart til uttrykk i en felles uttalelse fra Personvernrådet og EUs datatilsyn fra 14. januar i år,[187] der de to aktørene adresserer motstriden mellom Kommisjonens forslag til nye standardiserte personvernbestemmelser og Personvernrådets veileder. I denne sammenheng vises det til nettopp det poeng at det i vurderingen av tredjestatens beskyttelsesnivå først og fremst er relevant å se hen til om tredjestatens nasjonale lovgivning i det hele tatt tillater innsyn fra

[186] Se Annex to the Draft implementing decision (2020) s. 13.
[187] EDPB - EDPS Joint Opinion 2/2021.

offentlige myndigheter på en måte som strider mot EU-retten, og at det i forlengelsen av dette ikke er behov for å vurdere de praktiske erfaringene med innsynsbegjæringer fra myndighetshold.[188] Personvernrådet og EUs datatilsyn anbefaler derfor Kommisjonen å endre klausul 2 bokstav b punkt (i) slik at Kommisjonens forslag samsvarer med Personvernrådets veileder, og ikke gir rom for at subjektive faktorer tas med i vurderingen.[189]

Dersom denne motstriden fortsatt er til stede etter endelig vedtakelse av Personvernrådets veileder og Kommisjonens standardiserte personvernbestemmelser, må veilederen vike.[190] Som nevnt under oppgavens punkt 1.3, er kommisjonsbeslutninger etter TEUV artikkel 291 nr. 2 bindende, noe som ikke er tilfellet for Personvernrådets uttalelser.

[188] EDPB - EDPS Joint Opinion 2/2021 s. 19-20, avsnitt 87.
[189] EDPB - EDPS Joint Opinion 2/2021 s. 19 avsnitt 86.
[190] Praktiske erfaringer med innsynsforespørsler fra mottakerstatens myndigheter er også relevante etter Kommisjonens vedtak av 4. juni 2021. I del III, klausul 14 bokstav a og b i de nye standardiserte personvernbestemmelsene, pålegges partene de samme pliktene som etter forslagets klausul 2 bokstav a og b. I en fotnote til den nye klausul 14 bokstav b punkt (ii) presiserer Kommisjonen at et relevant moment ved vurderingen av mottakerstatens lovgivning og praksis er «relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame» (se Annex to the Commission Implementing Decision (2021) s. 22-23, fotnote 12). Praktiske erfaringer med innsynsforespørsler fra mottakerstatens myndigheter nevnes også som relevant i fortalepunkt 20 i Kommisjonens vedtak, se Commission Implementing Decision (2021) s. 5-6. Anmodningen fra Personvernrådet og EUs datatilsyn om å ikke gi rom for det de kaller subjektive faktorer er med andre ord ikke tatt til følge av Kommisjonen.

# 8 Konklusjon og konsekvenser

## 8.1 Gjelder det en risikobasert tilnærming ved overføring av personopplysninger til tredjestater?

Verken ordlyden i GDPR eller EU-domstolen gir klare svar på om det gjelder en risikobasert tilnærming ved overføring av personopplysninger til tredjestater, eller om Personvernrådets rettighetsbaserte tilnærming skal legges til grunn. Bestemmelsene i GDPR kapittel IV gjør det klart at forordningen ikke krever at risikoen for personvernbrudd er lik null. En samlet lesning av bestemmelsene i GDPR kapittel V, sammenholdt med EU-domstolens presiseringer i de to Schrems-avgjørelsene, gjør det videre klart at det må foreligge et beskyttelsesnivå som *i det vesentlige* tilsvarer det som gjelder ellers i forordningen. Som redegjort for under punkt 3.6, kan imidlertid ikke dette isolert sett resultere i at de risikobaserte bestemmelsene i kapittel IV får like stor betydning ved overføringer til tredjestater.

Etter en nærmere gjennomgang av GDPRs oppbygning og funksjon som en meta-regulering, gir imidlertid forordningen implisitte svar. Et av hovedpoengene med innføringen av ansvarsprinsippet og introduksjonen av de risikobaserte bestemmelsene i kapittel IV, var å la den behandlingsansvarlige kalibrere sine forpliktelser på en effektiv måte, og dermed sørge for bedre beskyttelse av de registrertes rettigheter totalt sett. Dette poenget gjør seg vel så mye gjeldende ved overføring av personopplysninger til tredjestater. De konkrete omstendighetene ved de utallige overføringene som daglig finner sted varierer i stor grad, noe som bør gjenspeiles i beskyttelsestiltakene. Personvernrådets rettighetsbaserte tilnærming, der sannsynlighetsbetraktninger ikke er relevant, kan på sin side resultere i en slik «box-ticking»-praksis som den økte ansvarliggjøringen i GDPR var ment å motvirke.

Når en i tråd med EU-rettslig metode leser GDPR i lys av pakten, kommer rasjonalet bak en risikobasert tilnærming enda tydeligere fram. Som redegjort for under punkt 4.3, forutsetter proporsjonalitetsprinsippet sammenholdt med friheten til å drive forretningsvirksomhet, jf. henholdsvis artikkel 52 og artikkel 16 i pakten, at det tas hensyn til den konkrete risikoen ved overføringen ved spørsmål om hvilke beskyttelsestiltak som gir tilstrekkelig beskyttelse.

En slik tolkning av GDPR tilfredsstiller også det EU-rettslige prinsippet om formålsrettet tolkning. Den risikobaserte tilnærmingen er best egnet til å ivareta forordningens to hovedformål, nemlig personopplysningsvernet og hensynet til fri utveksling av personopplysninger, jf. GDPR artikkel 1. Dersom den konkrete risikoen ikke er relevant, vil sistnevnte formål undergraves. Personopplysningsvernet vil på sin side ikke undergraves *med* en risikobasert tilnærming, ettersom denne tilnærmingen sørger for et vern som er proporsjonalt med det konkrete risikonivået.

I tillegg til dette er det elementer i premissene i Schrems II-dommen som ikke er forenlig med Personvernrådets uttalelser i veilederen om implementering av supplerende beskyttelsestiltak. Mens Personvernrådets tilnærming i realiteten innebærer at den eneste relevante faktoren er om tredjestatens lovgivning gir mottakeren av personopplysningene plikter som kolliderer med innholdet i overføringsgrunnlaget, gir EU-domstolen anvisning på en vurdering av *alle omstendighetene ved overføringen*. Som Kommisjonen legger til grunn i sitt forslag til nye standardiserte personvernbestemmelser, kan erfaringene med innsynsforespørsler fra mottakerstatens myndigheter i denne sammenheng være en relevant omstendighet.

Den rettighetsbaserte tilnærmingen som Personvernrådet legger til grunn, der sannsynlighetsbetraktninger anses som irrelevant ved vurderingen av beskyttelsesnivået ved overføring av personopplysninger til tredjestater, fremstår etter dette ikke holdbar i lys av det øvrige rettskildegrunnlaget. Personvernrådet virker å miste av syne at GDPR er implementert som en del av det store og komplekse rettskildebildet som EU-retten innebærer, der en rekke interesser må balanseres mot hverandre. Med Personvernrådets manglende hensyntagen til prinsippet som av denne grunn gjennomsyrer hele EU-retten – proporsjonalitetsprinsippet – kan en slik balanse vanskelig oppnås.

Ettersom sannsynlighetsbetraktninger omtales som *subjektive faktorer* i veilederen om supplerende beskyttelsestiltak,[191] kan uttalelsen her potensielt forstås som et forsøk på å motvirke sprikende praksis rundt vurderingen av hvilke beskyttelsestiltak som anses som egnede. Som det fremgår av fortalepunkt 76 i GDPR, bør risikoen «vurderes ut fra en objektiv vurdering der det fastslås om behandlingen av personopplysningene innebærer en risiko eller en høy risiko» (egen utheving).

[191] EDPB Recommendations 01/2020 avsnitt 42.

Samtidig kan det diskuteres hvorvidt det er treffende å omtale sannsynligheten for at tredjestatens myndigheter får innsyn i de aktuelle personopplysningene som en ren subjektiv faktor. Som påpekt av Rubinstein og Margulies, kan slike sannsynlighetsbetraktninger tvert imot anses som en objektiv faktor som man med rimelighet kan identifisere gjennom å se på praktiske erfaringer med innsynsbegjæringer fra den aktuelle staten.[192] For eksempel har det amerikanske handelsdepartementet publisert en rapport der det fremgår at den faktiske forekomsten av innsynsforespørsler fra amerikanske overvåkningsmyndigheter er lav.[193] Her er det naturligvis grunnlag for å så tvil rundt departementets habilitet, men poenget er fortsatt det samme. Som et forslag til en praktisk løsning i denne sammenheng, etterspør tenketanken CIPL en database med de risikovurderingene som er foretatt i forbindelse med overføring av personopplysninger ut av EU/EØS, slik at overføringene kan skje på en konsekvent måte.[194]

Uansett er det etter en samlet gjennomgang av de aktuelle rettskildene grunnlag for å konkludere med at overføringens risiko, herunder blant annet sannsynligheten for at tredjestatens myndigheter får innsyn i de overførte personopplysningene, er relevant ved overføring av personopplysninger til tredjestater. Det må med andre ord legges til grunn en risikobasert tilnærming til kravet om supplerende beskyttelsestiltak ved slike overføringer.

## 8.2 Hva er de nærmere konsekvensene av en risikobasert tilnærming ved overføring av personopplysninger til tredjestater?

Etter Schrems II-dommen er det klart at de standardiserte personvernbestemmelsene vedtatt av Kommisjonen i tråd med GDPR artikkel 46 nr. 2 bokstav c, ikke alene gir tilstrekkelig beskyttelse ved overføring av personopplysninger til tredjestater som ikke opprettholder et adekvat beskyttelsesnivå. Som vi har sett, innebærer imidlertid ikke dette en helt binær tilnærming til kravet om supplerende beskyttelsestiltak, der en gitt type tiltak enten anses som effektive eller ineffektive. Dersom beskyttelsesnivået i tredjestaten uten noen beskyttelsestiltak ikke er tilfredsstillende, må det foretas en differensiert vurdering av hvilke tiltak som *i den konkrete saken* må implementeres for å oppnå et tilfredsstillende

[192] Rubinstein og Margulies (2021) s. 27.
[193] U.S Government (2020).
[194] CIPL (2020).

beskyttelsesnivå *med* supplerende tiltak. Formålet i det følgende er å gi en overordnet og ikke uttømmende redegjørelse for ulike momenter eksportøren bør ta hensyn til i denne sammenheng, med utgangspunkt i det som allerede er sagt om systemet i GDPR.

I tråd med ansvarsprinsippet i forordningens artikkel 5 nr. 2 må den behandlingsansvarlige ta utgangspunkt i de vurderinger det gis anvisning på i artikkel 24 nr. 1 i forbindelse med valg av beskyttelsestiltak. Dersom det er en databehandler som skal stå for overføringen, må tilsvarende vurderinger uansett foretas ved valget av databehandler, jf. GDPR artikkel 28 nr. 1, all den tid involvering av en databehandler i seg selv utgjør en risiko. Denne vurderingen må behandlingsansvarlig se i sammenheng med reglene i artikkel 25 og 35.[195] Det generelle kravet om gjennomføring av egnede beskyttelsestiltak gjelder uansett vel så mye for databehandleren som for behandlingsansvarlig, jf. artikkel 32 nr. 1.

Ved vurderingen av «risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter», jf. artikkel 24 nr. 1, må det i forbindelse med spørsmålet om alvorlighetsgraden av de potensielle konsekvensene for det første tas hensyn til arten av de aktuelle personopplysningene. Dersom det eksempelvis dreier seg om slike sensitive opplysninger som listes opp i GDPR artikkel 9 nr. 1, tilsier det at det dreier seg om en overføring av høy risiko. I tråd med punkt 75 i GDPRs fortale gjelder det samme for opplysninger som på annen måte kan medføre store negative konsekvenser for den registrerte, slik som identitetstyveri eller tap av konfidensialitet for taushetsbelagte personopplysninger, dersom de kommer i myndighetenes besittelse på en måte som er i strid med GDPR. I slike tilfeller er det gode grunner for å kreve at beskyttelsestiltakene så langt det lar seg gjøre må gjøre tilgang for tredjestatens myndigheter umulig eller ineffektiv, typisk gjennom sterke krypteringsløsninger.

Det er viktig å presisere at en risikobasert tilnærming ikke skal gå på bekostning av personvernet, men at den heller skal åpne for mer adekvate tiltak. Selv om det ikke dreier seg om opplysninger som i seg selv medfører alvorlige konsekvenser for den registrerte dersom de kommer på avveie, er det derfor fortsatt grunn til å utvise varsomhet ved vektlegging av lav sannsynlighet for innsynsbegjæringer fra tredjestatens myndigheter. For vurderingen av overføringens alvorlighetsgrad må det nemlig også være relevant å se hen til det generelle beskyttelsesnivået i den aktuelle tredjestaten. Som nevnt under punkt 1.4, er det en stor

[195] Jarbekk mfl. (2019) s. 270-271.

utfordring for både små og store bedrifter å foreta slike landrisikovurderinger. Dersom det imidlertid skulle avdekkes nærmere detaljer om det generelle beskyttelsesnivået i mottakerstaten, vil det kunne gi bedre oversikt over det totale risikobildet. Både etter Snowden-avsløringene og etter de to Schrems-sakene for EU-domstolen er beskyttelsesnivået i USA eksempelvis nøye behandlet. Her har man blant annet funnet at amerikansk lovgivning ikke gir europeiske borgere slik domstolsadgang som kreves etter artikkel 47 i pakten.[196] Det er med andre ord en grunnleggende rettighet som står på spill, med den konsekvens at alvorlighetsgraden ved et eventuelt GDPR-stridig innsyn i de aktuelle opplysningene fortsatt er relativt høy. Det kan i denne sammenheng vises til fortalepunkt 75 hver det nevnes tilfeller der «de registrerte kan bli fratatt sine rettigheter og friheter» som en særlig relevant konsekvens ved risikovurderingen.[197] I slike tilfeller må det i så fall kreves svært lav sannsynlighet for at myndighetene vil kreve tilgang, for at det samlede risikonivået kan anses for å være lavt nok til at andre tiltak en sterk kryptering er nok.

Det kan imidlertid tenkes at det vil komme rapporter om rettstilstanden i andre tredjestater i tiden som kommer, der man finner at beskyttelsesnivået ikke er adekvat, men fortsatt bedre enn det som gjelder i USA. Et eksempel kan være at den aktuelle tredjestaten har uproporsjonale overvåkningshjemler, men at den gir den europeiske borgeren, som personopplysningene knytter seg til, tilgang til effektive rettsmidler.[198] I så fall er alvorlighetsgraden ved overføringen mindre, med den konsekvens at kravet til sannsynlighet ikke behøver å være like strengt.

Hva gjelder sannsynlighetsvurderingen, er det blant annet relevant å se hen til databehandlerens praktiske erfaringer med innsynsforespørsler for den aktuelle typen personopplysninger fra mottakerstaten. Dersom myndighetene i denne staten flere ganger tidligere har kommet med slike forespørsler, taler det for at sannsynligheten for uberettiget innsyn er høy, hvilket i sin tur påvirker risikoen ved overføringen i negativ retning.

Blant annet med utgangspunkt i de momentene som er nevnt over her, er det mulig for dataeksportører å avgjøre – før supplerende tiltak implementeres – hvorvidt risikoen ved den konkrete overføringen er lav, moderat eller høy, for så å kunne ta stilling til hvilke

[196] Se for eksempel C-311/18 *Schrems II,* avsnitt 149.
[197] Ivaretakelsen av disse rettighetene fremgår også av GDPR artikkel 46.
[198] Foss (2021) under punkt «Verden sett i lys av Schrems II», der artikkelforfatteren antyder at slike effektive rettsmidler kan oppnås i India.

beskyttelsestiltak som er egnet til å redusere risikoen til et tilfredsstillende nivå. Jo høyere risiko, jo større behov er det for sterke tekniske tiltak som er egnet til å gjøre tredjestatens myndigheters adgang til personopplysningene umulig eller ineffektiv. Motsetningsvis vil mulighetene for å kun forholde seg til kontraktsrettslige, organisatoriske eller lettere tekniske tiltak være større desto lavere risiko overføringen fører med seg. Uansett er det verdt å merke seg at dataeksportørens risikovurderinger og påfølgende konklusjoner må dokumenteres, slik ansvarsprinsippet i GDPR artikkel 5 nr. 2 krever.

# 9 Rettspolitiske betraktninger – spenningen mellom personvernet og den teknologiske utviklingen

## 9.1 Internettet forholder seg ikke til landegrenser

Som nevnt innledningsvis under punkt 1.1, er datadrevet økonomi ansett som en sentral faktor for videre økonomisk vekst, både nasjonalt og globalt. Problematikken i Schrems II-dommen illustrerer godt de store utfordringene vi står overfor i denne sammenheng. Oppgaven har vist at det er vanskelig å opprettholde et fullgodt personopplysningsvern og samtidig holde følge med den teknologiske utviklingen. Den rettighetsbaserte tilnærmingen som Personvernrådet og EUs datatilsyn tilsynelatende legger til grunn, innebærer for eksempel at man er nødt til å si fra seg en rekke av de ressursbesparende skytjenestetilbudene som vi drar nytte av i dag. Også med en risikobasert tilnærming lagt til grunn, er det per dags dato vanskelig å opprettholde tempoet i dagens utvikling. USAs nevnte overvåkningspraksis utgjør i seg selv en merkbar risiko for europeiske borgeres personvern. Enkelte potensielle overføringer vil derfor ikke være lovlige etter en nødvendig risikovurdering.

Den vanskelige balansegangen mellom personvern og teknologisk utvikling kan blant annet forstås som en konsekvens av at teknologien, og herunder særlig internettet, ikke forholder seg til landegrenser. I løpet av få sekunder kan man fra en datamaskin i Norge lagre opplysninger på skybaserte servere i USA, der dokumentet under overføringen fraktes via en rekke andre land. For å være tilgjengelig til alle døgnets tider, kan det i tillegg tenkes at tjenestetilbyderen har kundeservicesentre i India, som gis fjerntilgang til de aktuelle opplysningene.

Som fremhevet av Hörnle, er imidlertid en forutsetning for rettslig regulering at det foreligger *jurisdiksjon*[199] – kompetanse til å gi lover og regler og håndheve dem.[200] For eksempel har EUs medlemsstater gitt EU-domstolen jurisdiksjon til å avgjøre tvister om EU-rettslige

[199] Hörnle (2021a).
[200] Hörnle (2021) s. 4.

spørsmål, jf. TEU artikkel 19 nr. 1. Det finnes imidlertid ingen felles personvernregler som gjelder på tvers av alle kontinenter, og dermed heller ingen overnasjonal domstol som kan avgjøre spørsmål om personvern i USA eller India den ene dagen, og i Europa den andre. Dette gjør det vanskelig å gi og håndheve regler som effektivt beskytter de aktuelle personopplysningene på deres reise gjennom verden.[201]

Utfordringen er med andre ord hvordan en kan komme seg forbi disse utfordringene knyttet til jurisdiksjon, og samtidig oppnå tilstrekkelig ivaretakelse av borgernes personvern. Med skytjenesteteknologiens sentrale posisjon i både dagens og fremtidens datadrevne økonomi, er det vanskelig å se for seg en reversering av den pågående utviklingen av hensyn til nettopp personvernet. Ettersom utviklingen av ny teknologi i første rekke kommer fra USA og Asia,[202] er det også vanskelig å se for seg at det europeiske skytjenestetilbudet i overskuelig fremtid vil befinne seg på et nivå som gjør det unødvendig med overføring av personopplysninger ut av EU/EØS. Spørsmålet da blir om det kan identifiseres andre løsninger på kort eller lang sikt som kan gjøre balansegangen mellom et tilfredsstillende personvern og deltakelse i den teknologiske utviklingen mulig.

I relasjon til dette skal det under punkt 9.2 knyttes noen særskilte betraktninger til i hvilken grad den risikobaserte tilnærmingen er egnet til å bøte på noen av problemene knyttet til reguleringen av personvernet på tvers av kontinenter. Videre har oppgaven vist at tekniske beskyttelsestiltak spiller en sentral rolle når personopplysninger skal beskyttes mot innsyn fra fremmede myndigheter. Derfor vil det i punkt 9.3 ses nærmere på de store teknologiselskapenes rolle ved ivaretakelsen av borgernes personvern. Med utgangspunkt i det som er sagt i punktene 9.1-9.3, samt ellers i oppgaven, vil det til slutt i punkt 9.4 knyttes noen avsluttende betraktninger til hvilke mulige løsninger vi kan se for oss både på kort og lang sikt.

## 9.2 Kan den risikobaserte tilnærmingen være løsningen?

En mulig løsning på utfordringene med internettets grenseløse karakter og manglende jurisdiksjon er ifølge Hörnle *selvregulering*, nærmere bestemt at bedrifter selv bestemmer

[201] En sak fra norsk rett som ikke dreier seg om personvern, men som likevel illustrerer utfordringene med internett og jurisdiksjon godt, er Tidal-saken inntatt i HR-2019-610-A, der Høyesterett tok stilling til om datamateriale lagret på utenlandske servere kunne brukes som bevismateriale i en norsk straffesak. Saken er nærmere kommentert av Jon Petter Rui i artikkelen *Høyesterett i «skyen»* i Lov og Rett 05/2019 (Volum 58).
[202] Se punkt 4.3 i denne oppgaven.

reglene på enkelte områder.[203] I et personvernperspektiv er det aktuelt å se tilbake til betraktningene om GDPR som en meta-regulering, der det legges opp til at bedriftene selv avgjør hvilke tiltak som er egnet for å nå de regulatoriske målene, med utgangspunkt i risikovurderinger. Denne risikobaserte tilnærmingen legger opp til en balansering av hensynene til personopplysningsvern og fri utveksling av personopplysninger, og dermed også hensynet til den teknologiske utviklingen. På denne måten tvinges bedrifter til å ta stilling til beskyttelsesnivået i aktuelle mottakerstater utenfor EU/EØS, hvilket til en viss grad kan bøte på manglende regulering på tvers av kontinenter.

Meta-regulering og den risikobaserte tilnærmingen har imidlertid også sine åpenbare svakheter. Særlig relevant er hvordan meta-regulering som lovgivningsmekanisme er svært tillitsbasert, og fordrer at bedrifter handler i god tro og med mål om å nå de regulatoriske målene. Selv om det av markedsføringshensyn er gode grunner for en bedrift til å fremstå som om den tar personvern på alvor, er det ikke til å komme bort fra at bedriftenes økonomiske incentiver til å i ond tro utnytte seg av det skjønnet de har blitt tildelt, er tilstedeværende. For små og mellomstore bedrifter med lite kapital vil det eksempelvis være fristende å benytte billige skyløsninger utenfor EU/EØS, som til gjengjeld ikke nødvendigvis kan garantere et adekvat beskyttelsesnivå.

Bedriftenes økonomiske incentiver til å misbruke sitt skjønn etter GDPR er riktignok forsøkt motvirket med de høye bøtesatsene ved brudd. Etter forordningens artikkel 83 nr. 5 bokstav c skal det ved overtredelser av bestemmelsene om overføring av personopplysninger til tredjestater ilegges overtredelsesgebyr på opptil 20 000 000 euro eller, dersom det dreier seg om et foretak, opptil 4 % av den samlede globale omsetningen, dersom dette beløpet er høyere. Dette er naturligvis godt egnet til å virke avskrekkende for bedrifter som er fristet til å misbruke sitt skjønn.

Samtidig forutsetter bøtesystemet at overtredelser av GDPR gjennomgående følges opp av datatilsynene. På grunn av datatilsynenes begrensede kapasitet, er det vanskelig å oppfylle denne forutsetningen. Kritikken fra Maximilian Schrems rettet mot det irske datatilsynets påståtte manglende håndheving av GDPR generelt, og Schrems II-dommen spesielt, er et eksempel på dette. I en tale til det irske parlamentet i april i år, viste Schrems til at datatilsynet i løpet av året kun har sett for seg å behandle mellom seks og syv av de 10 000 klagene det

[203] Hörnle (2021a).

har mottatt.[204] Ettersom en rekke av de store teknologiselskapene har sine europeiske hovedkvarter i Irland, er det irske datatilsynet en viktig håndhever av GDPR.[205] Med en slik statistikk lagt til grunn, er det klart at bøtesystemet har sine mangler. Debatten mellom Schrems og lederen for det irske datatilsynet, Helen Dixon, har vært opphetet, og Dixon har riktignok kalt Schrems' påstand forenklet og overfladisk.[206] Uten at det skal tas nærmere stilling til denne debatten her, illustrerer den uansett poenget. Håndhevingsfunksjonen som de nasjonale datatilsynene er tillagt, med det bøtesystemet som følger med, er ikke i seg selv nok til at den risikobaserte tilnærmingen kan anses for å løse de jurisdiksjonsrelaterte utfordringene med ivaretakelsen av personvernet.[207]

Som fremhevet av Julia Black, kan man ikke fra lovgiverhold håpe på at den risikobaserte tilnærmingen på mirakuløst vis løser de regulatoriske utfordringene man står overfor.[208] Ved implementeringen av en slik tilnærming må man derfor også anerkjenne og ta hensyn til dens begrensninger. For oppgavens tema innebærer dette nærmere bestemt at dataeksportørers risikovurderinger ikke alene kan bøte på de utfordringene man står overfor når personopplysninger overføres på tvers av kontinenter. Dersom man får en mer brukervennlig og samtidig sikker krypteringsteknologi, kan imidlertid disse risikovurderingene lettere resultere i en konklusjon i retning av at overføringen er lovlig.

## 9.3 Hva kan tjenesteleverandørene bidra med?

Selv om det i tråd med GDPR artikkel 5 nr. 2 er den behandlingsansvarlige som har ansvaret for at personvernprinsippene overholdes og at den registrertes rettigheter og friheter beskyttes, er det for den gjengse behandlingsansvarlige bedrift vanskelig å påvirke praksisen rundt overføring av personopplysninger til tredjestater i en mer personvernvennlig retning. Behandlingsansvarlige bedrifter har ofte dårlige forhandlingskort når databehandleravtaler i

[204] https://www.independent.ie/business/technology/max-schrems-and-helen-dixon-clash-over-irish-gdpr-enforcement-on-big-tech-40363344.html (sist lest 04.05.2021).
[205] https://www.irishtimes.com/business/technology/irish-approach-to-data-protection-kafkaesque-says-schrems-1.4533257 (sist lest 05.05.2021).
[206] https://www.independent.ie/business/technology/max-schrems-and-helen-dixon-clash-over-irish-gdpr-enforcement-on-big-tech-40363344.html (sist lest 04.05.2021).
[207] I sin resolusjon av 21. mai 2021 (2021/2594(RSP)) uttrykte Europaparlamentet for øvrig bekymring tilknyttet det britiske datatilsynets manglende håndheving av GDPR, og viste til at datatilsynet først og fremst benyttet sine håndhevingsmekanismer i de mest alvorlige sakene. Resolusjonen tok for seg den ventede adekvansbeslutningen for Storbritannia, og er tilgjengelig her: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0262_EN.html (se særlig under overskriften «Enforcement of the GDPR») (sist lest 31.05.2021).
[208] Black (2010) s. 222.

medhold av GDPR artikkel 28 skal inngås, og står dermed sjeldent i en posisjon der det kan stilles strenge krav til beskyttelse av de registrertes personopplysninger. Det er først og fremst de ledende leverandørene av skytjenester, deriblant de såkalte «Big Tech»-selskapene Google, Apple, Amazon, Facebook og Microsoft,[209] som har ressursene, kompetansen og patentene til å for eksempel utvikle nye krypteringsløsninger.[210] Følgelig er det disse aktørene – som gjerne opptrer som databehandlere – som står i posisjon til å styre markedet i retning av et styrket personvern.

At det er vanskelig for behandlingsansvarlige å stille strenge krav, også der den behandlingsansvarlige er en i utgangspunktet innflytelsesrik aktør, kan illustreres ved etterforskningen EUs datatilsyn gjorde av EU-institusjonenes bruk av Microsofts Irelands tjenester. Microsofts databehandling innebar blant annet at en rekke av EU-institusjonenes personopplysninger ble overført til det USA-baserte morselskapet Microsoft Corporation, samt til underleverandører i en rekke tredjestater.[211] Datatilsynet fant i denne sammenheng blant annet at databehandleravtalen verken var egnet til å gi oversikt over hvilke overføringer som ville finne sted,[212] eller hvilke beskyttelsestiltak som eventuelt skulle implementeres for de ulike overføringene.[213] I forlengelsen av dette ble det vist til at det i de standardiserte personvernbestemmelsene – som ble brukt som overføringsgrunnlag – skal gis en grundig spesifisering av forholdene rundt de ulike overføringene,[214] men at Microsoft snarere hadde forhåndsutfylt generiske beskrivelser ment å passe alle kunder.[215] Innholdet i disse bestemmelsene var snarere noe som ble pålagt av Microsoft, enn et resultat av forhandlinger mellom partene.[216]

Databehandlere er også forpliktet til GDPR, og det er vel så mye i deres interesse at tjenestene de tilbyr innebærer et beskyttelsesnivå i tråd med det forordningen krever. At de fleste behandlingsansvarlige bedrifter ikke står i posisjon til å påvirke praksisen tilknyttet overføring av personopplysninger til tredjestater, trenger med andre ord ikke å resultere i en

[209] https://www.globaldata.com/big-tech-to-take-an-ever-larger-piece-of-the-cloud-computing-pie-says-globaldata/ (sist lest 08.05.2021).
[210] https://www.forbes.com/sites/forbestechcouncil/2021/01/07/encryption-isnt-the-problem-its-the-solution/?sh=40827ef51e89 (sist lest 07.05.2021).
[211] EDPS Public Paper *on Outcome of own-initiative investigation into EU institutions' use of Microsoft products and services* (2020) s. 104.
[212] EDPS Public Paper (2020) s. 107.
[213] EDPS Public Paper (2020) s. 108.
[214] EDPS Public Paper (2020) s. 111.
[215] EDPS Public Paper (2020) s. 112.
[216] EDPS Public Paper (2020) s. 113.

status quo-situasjon. Poenget med å fremheve databehandlernes posisjon er tvert imot å vise at Schrems II-dommen kan være egnet til å tvinge de store teknologileverandørene til å iverksette tiltak som gir en bedre beskyttelse av europeiske borgeres personopplysninger.

Slike tiltak kan for det første bestå i å flytte datasentre til Europa, og dermed begrense antallet overføringer av personopplysninger ut av EU/EØS. Relevant i denne sammenheng er Microsofts nylige[217] annonsering av planen «EU Data Boundary for the Microsoft Cloud», der det settes som mål at all lagring og prosessering gjennom Microsofts skytjenester innen slutten av 2022 skal skje i Europa.[218] Dette vil naturligvis senke det generelle behovet for overføring av personopplysninger til tredjestater betraktelig, særlig hvis andre skytjenestetilbydere gjør det samme. I hvilken grad dette vil redusere risikoen for tredjestaters innsyn i europeiske borgeres personopplysninger, kan riktignok diskuteres. Som nevnt under punkt 1.4, er en særskilt problemstilling hva som skjer der en databehandler i EU/EØS er underlagt overvåkningslover i en tredjestat. Selv om selskaper som Microsoft sørger for at all lagring og prosessering skjer innenfor EU/EØS, kan de for eksempel fortsatt være underlagt amerikanske overvåkningslover slik som FISA 702 eller CLOUD Act.[219] Oppgaven avgrenser som nevnt mot en nærmere behandling av denne problemstillingen. Poenget i denne sammenheng er imidlertid å presisere at virkningene av Microsofts nylig annonserte planer ikke nødvendigvis skal overdrives.

I tillegg til å flytte databehandlingsaktivitetene til Europa, kan teknologiselskapene også bidra ved å utnytte sin kompetanse til å utvikle nye tekniske løsninger som gjør det tryggere å behandle data i tredjestater. For eksempel samarbeider noen av verdens største teknologiselskaper, inkludert Facebook, Google, Microsoft, Alibaba og IBM, gjennom stiftelsen Confidential Computing Consortium om å utvikle krypteringsmetoden *Confidential Computing*.[220] Metoden innebærer grovt skissert at det kun er en autorisert krets av aktører som kan få tilgang til de aktuelle personopplysningene i dekryptert versjon.[221] På denne måten kan kunden behandle data som er lagret på skybaserte servere basert i en tredjestat, samtidig som dataene er kryptert for skytjenesteleverandøren. Dermed kommer ikke tredjestatens

[217] Planen ble annonsert 6. mai i år.
[218] https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/?mkt_tok=MTM4LUVaTS0wNDIAAAF85AM0yBfDrIhKdTsRLGap1ABfu6H6VI-uA7dgbrLJsTt2q4-S9TfLMCo1tzq7wK9pZejgr33KGQGxkFAp5DXDKm2oTuBTWNPjkVEYuIJAIlZ (sist lest 20.05.2021).
[219] Datatilsynet (2020a).
[220] Se https://confidentialcomputing.io/members/ for oversikt over stiftelsens medlemmer (sist lest 20.05.2021).
[221] https://searchcloudcomputing.techtarget.com/definition/confidential-computing (sist lest 20.05.2021).

myndigheter noen vei ved eventuelle pålegg rettet mot dataeksportøren om å få de aktuelle personopplysningene tilgjengeliggjort.

Confidential Computing er imidlertid kun egnet til å minimere risikoen for innsyn fra tredjestatens myndigheter der tjenesten av natur ikke krever at databehandleren har tilgang til de overførte personopplysningene. Der den aktuelle tjenesten derimot innebærer at databehandleren selv behandler datasettet, er denne krypteringsløsningen lite egnet. Som nevnt under punkt 4.3, finnes det per i dag ingen utbredte løsninger som gjør det mulig å behandle data, for eksempel i form av å redigere datafelt eller å slette eller legge til opplysninger, dersom det aktuelle datasettet er kryptert.

Slik teknologi, kalt *homomorfisk kryptering*, er imidlertid under utvikling.[222] For øyeblikket er denne krypteringsmetoden ikke tilstrekkelig utviklet til at den muliggjør ytelser på et tilfredsstillende nivå, men det er grunn til tro på progresjon her.[223] Når slik teknologi er på plass, vil beskyttelsen av personopplysninger overført ut av EU/EØS være på et langt høyere nivå.

Parallelt med den teknologiske utviklingen vil det med andre ord være flere og flere databehandlingsaktiviteter som lar seg utføre i tredjestater, uten at tredjestatens myndigheter kan kreve innsyn i de overførte personopplysningene. Dersom det samtidig legges til rette for at en større andel av dagens databehandlingstjenester holdes innenfor EU/EØS, er det klart at teknologiselskapenes praksis kan ha stor innflytelse på beskyttelsesnivået tilknyttet europeiske borgeres personopplysninger.

## 9.4 Veien videre – hvilke løsninger kan vi se etter på kort og lang sikt?

De foregående punktene har vist at den risikobaserte tilnærmingen klart nok ikke alene kan være løsningen på utfordringene som følger av internettets grenseløse karakter. Gjennom teknologisk utvikling kan vi imidlertid i det lange løp håpe på tekniske løsninger som tillater at flere og flere databehandlingsaktiviteter utføres i tredjestater, uten at tredjestatens myndigheter kan kreve innsyn i de overførte personopplysningene. Slik teknologi kan igjen

[222] https://www.microsoft.com/en-us/research/project/homomorphic-encryption/ (sist lest 20.05.2021).
[223] Datatilsynet (2018a).

gjøre det mulig å fullt ut nå målene om fri utveksling av personopplysninger, samtidig som beskyttelsen av de registrertes rettigheter og friheter gjennomgående er på et tilfredsstillende nivå. Inntil disse tekniske løsningene er på plass, er det risikovurderinger og mest mulig lagring og databehandling i Europa som er det kortsiktige svaret på utfordringene knyttet til spenningen mellom personvernet og den teknologiske utviklingen.

Det kan imidlertid hevdes at de langsiktige løsningene ikke bør innebære at man er prisgitt private aktørers innovasjon. Det er ingen garanti for at helt tilfredsstillende løsninger kommer på markedet, og risikoen for datainnbrudd fra både private aktører og overvåkningsmyndigheter vil alltid være til stede. Som et siste alternativ til løsning på utfordringene med å regulere den teknologiske utviklingen, bør man derfor håpe på større enighet om beskyttelsesnivå på tvers av kontinentene. Den harde fronten fra EU-hold i forbindelse med overføring av personopplysninger til tredjestater kan potensielt forstås i lys av dette, i den forstand at man forsøker å påvirke USA og andre stater i en mer personvernvennlig retning. Den nærmest umulige balansegangen mellom å dra nytte av den teknologiske utviklingen og samtidig verne om personopplysningene gjør det naturligvis både ønskelig og viktig at stater både i og utenfor Europa tar personvernet på alvor.

Dersom EU kan bruke sin viktige rolle i verdensøkonomien til å påvirke andre stater i en slik retning, er det vel og bra. Som denne oppgaven har vist, er imidlertid baksiden av medaljen ved et slikt politisk spill at det er de europeiske bedriftene som risikerer å bære kostnadene. Uansett kan det nevnes at EU og USA for øyeblikket forhandler om en ny transatlantisk overføringsmekanisme, som er ment å skulle være i tråd med kravene etter Schrems II-dommen.[224] I lys av alt som er avdekket gjennom Snowden-avsløringene og de to Schrems-sakene, er det imidlertid grunn til å justere eventuelle forventninger om at en ny avtale kan gi tilfredsstillende vern. Med andre ord er det på ingen måte utenkelig at vi i fremtiden igjen vil vente på EU-domstolens avgjørelse etter et tredje søksmål fra Maximilian Schrems.

[224] European Commission – Statement – Intensifying Negotiations on transatlantic Data Privacy Flows: A Joint Press Statement by European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Gina Raimondo 25. Mars 2021 (https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_1443 (sist lest 12.04.2021)).

# 10 Litteraturliste

## 10.1 Lover


| | |
|---|---|
| Personopplysningsloven 2018 | Lov av 15. juni 2018 nr. 31 om behandling av personopplysninger (personopplysningsloven) |


## 10.2 Internasjonale traktater og konvensjoner


| | |
|---|---|
| EMK | Convention for the Protection of Human Rights and Fundamental Freedoms, Roma, 04.11.1950 (Den europeiske menneskerettighetskonvensjon) |
| Pakten | Charter of Fundamental Rights of the European Union OJ C 326, 26.10.2012, s. 391-407 (EUs pakt om grunnleggende rettigheter) |
| TEU | Traktaten om Den europeiske union, EUT OJ C 326, 26.10.2012 s. 1-390 |
| TEUV | Traktaten om Den europeiske unions virkemåte, EFT OJ C 326, 26.10.2012 s. 1-390 |


## 10.3 EUs sekundærlovgivning

### 10.3.1 Forordninger og direktiver


| | |
|---|---|
| Personvernforordningen | Europaparlaments- og rådsforordning (EU) 2016/579 av 27.4.2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike |

| | |
|---|---|
| | opplysninger samt om oppheving av direktiv 95/46/EF [GDPR], OJ L 119, 04.05.2016, s. 1-88 |
| Personverndirektivet | Europaparlaments- og rådsdirektiv 95/46/EF av 24.10.1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger, OJ L 281, 23.11.1995, s. 31-50 |

### 10.3.2 Beslutninger fra EU-kommisjonen

| | |
|---|---|
| Decision 2000/520/EC | Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ L 215, 25.8.2000, s. 7-47 |
| Decision 2001/497/EC | Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC, OJ L 181, 4.7.2001, s. 19-31 |
| Decision 2004/915/EC | Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, OJ L 385, 29.12.2004, s. 74-84 |
| Decision 2010/87/EU | Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third |

| | |
|---|---|
| | countries under Directive 95/46/EC of the European Parliament and of the Council, OJ L 39, 12.2.2010, s. 5-18 |
| Decision 2016/1250/EU | Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document (2016) 4176), OJ L 207, 1.8.2016, s. 1-112 |
| Draft implementing decision (2020) | European Commission Draft implementing decision on standard contractual clauses for the transfers of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council |
| Annex to the Draft implementing decision (2020) | Annex to the European Commission Draft implementing decision on standard contractual clauses for the transfers of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council |
| Implementing Decision (2021) | Commission Implementing Decision of 4.6.2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council |
| Annex to the Implementing | Annex to the Commission Implementing |

| | |
|---|---|
| Decision (2021) | Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council |

## 10.4 Rettspraksis fra EU-domstolen

| | |
|---|---|
| C-73/07 *Satakunnan Markkinapörssi* | Dom av 16. desember 2008, *Satakunnan Markkinapörssi,* ECLI:EU:C:2008:727 |
| C-402 og 432/07 *Sturgeon* | Dom av 19. november 2009, *Sturgeon and others*, ECLI:EU:C:2009:716 |
| C-424/10 og C-425/10 *Ziolkowski* | Dom av 21. desember 2011, *Ziolkowski og Szeja mfl.*, ECLI:EU:C:2011:866 |
| C-7/11 *Caronna* | Dom av 28. juni 2012, *Caronna*, ECLI:EU:C:2012:396 |
| C-480/10 *Kommisjonen mot Sverige* | Dom av 25. april 2013, *European Commission v Kingdom of Sweden*, ECLI:EU:C:2013:263 |
| C-345/13 *Karen Millen Fashion* | Dom av 19. juni 2014, *Karen Millen Fashions*, ECLI:EU:C:2014:2013 |
| C-362/14 *Schrems I* | Dom av 06. oktober 2015, *Schrems I,* ECLI:EU:C:2015:650 |
| C-311/18 *Schrems II* | Dom av 16. juli 2020, *Schrems II*, ECLI:EU:C:2020:559 |

## 10.5 Veiledere, uttalelser og rapporter fra EU-organer

| | |
|---|---|
| Art 29 WP, Opinion 1/98 | Article 29 Working Party, Opinion 1/98 «Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS)», 1998. [*Sitert* |

| | |
|---|---|
| | *etter Gellert, Raphaël, Why the GDPR risk-based approach is about compliance risk, and why it's not a bad thing, Radboud University, 2017 s. 5*] |
| Article 29 Working Party og Working party of Police and Justice (2009) | Article 29 Working Party and Working Police and Justice «The Future of Privacy: Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to the Protection of Personal Data», 2009. [*Sitert etter Gellert, Raphaël, The Risk Based Approach to Data Protection, Oxford, 2020 s. 158*] |
| European Commission COM/2010/0609 | Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union COM/2010/0609 (kan lastes ned her: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52010DC0609) |
| European Commission SEC/2012/0072 | Commission Staff Working Paper: Impact Assessment Accompanying the Document Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data SEC/2012/0072, 2012 (kan lastes ned her: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52012SC0072) |

| | |
|---|---|
| EDPS Position Paper (2014) | European Data Protection Supervisor, The transfer of personal data to third countries and international organisations by EU institutions and bodies, Position Paper, 14.07.2014 (kan lastes ned her: https://edps.europa.eu/sites/default/files/publication/14-07-14_transfer_third_countries_en.pdf) |
| A29WP Statement (2014) | Article 29 Working Party, Statement on the role of a risk-based approach in data protection legal frameworks, WP218, 2014 (kan lastes ned her: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf) |
| A29WP Guidelines (2017) | Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is «likely to result in a high risk» for the purposes of Regulation 2016/679, 04.04.2017 (kan lastes ned her: https://ec.europa.eu/newsroom/article29/items/611236) |

| | |
|---|---|
| EDPB Guidelines 2/2018 | EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25.05.2018 (kan lastes ned her: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf) |
| EDPB Recommendations 01/2020 | EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, 10.11.2020 (kan lastes ned her: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en) |
| EDPB Recommendations 02/2020 | EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, 10.11.2020. (kan lastes ned her: https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf) |
| European Commission COM/2020/103 | European Commission, Communication from the Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions, an SME Strategy for a sustainable and digital Europe, Brussel, 10.03.2020 (kan lastes ned her: https://ec.europa.eu/info/sites/default/files/communication-sme-strategy-march-2020_en.pdf) |
| European Commission (2020) | European Commission, The European data Market Monitoring 2020 (kan lastes ned her: https://digital- |

| | |
|---|---|
| | strategy.ec.europa.eu/en/library/european-data-market-study-update) |
| EDPS Public Paper (2020) | European Data Protection Supervisor, EDPS Public Paper on outcome of own-initiative investigation into EU institutions' use of Microsoft products and services 2020 (kan lastes ned her: https://edps.europa.eu/sites/default/files/publication/20-07-02_edps_euis_microsoft_contract_investigation_en.html) |
| EDPB-EDPS Joint Opinion 02/2021 | EDPB-EDPS Joint Opinion 02/2021 on standard contractual clauses for the transfer of personal data to third countries, 2021 (kan lastes ned her: https://edpb.europa.eu/system/files/2021-04/edpb_edps_joint_opinion_dgc_en.pdf) |

## 10.6 Juridisk litteratur

### 10.6.1 Bøker

| | |
|---|---|
| Aall (2011) | Aall, Jørgen, *Rettsstat og menneskerettigheter,* Fagbokforlaget 2011 |
| Black (2010) | Black, Julia, «Risk-based regulation: Choices, practises and lessons being learnt», *Risk and regulatory policy: Improving the governance of risk*, OECD (red.), OECD Publishing 2010, s. 185-236. [*Sitert etter Gellert, Raphaël, The risk based approach to data protection, Oxford 2020, s. 247*] |

| | |
|---|---|
| Fredriksen og Mathisen (2018) | Fredriksen, Halvard Haukeland, Mathisen, Gjermund, *EØS-rett*, 3. utgave, Fagbokforlaget 2018 |
| Gellert (2020) | Gellert, Raphaël, *The risk based approach to data protection*, Oxford 2020 |
| Hörnle (2021) | Hörnle, Julia, *Internet jurisdiction law and practice*, Oxford 2021 |
| Jarbekk (2019) | Jarbekk, Eva, Kaare M. Risung, Jeppe Songe-Møller, Inge Kristian Brodersen, Anne-Marit Wang Sandvik, Anette Øvrehus, Øivind K. Foss, Hedda Emilie Bratt, Christopher Thue Jerving og Johanne Førd, *Personopplysningsloven og personvernforordningen (GDPR) med kommentarer*, Gyldendal 2019 |
| Kuner, Bygrave og Docksey (2020) | Kuner, Christopher, Lee A. Bygrave, Christopher Docksey, *The General Data Protection Regulation: a commentary*, Oxford 2020 |
| Lynskey (2016) | Lynskey, Orla, *The foundations of EU data protection law,* Oxford University Press 2016. [*Sitert etter: Gellert, Raphaël, The risk based approach to data protection, Oxford 2020 s. 2*] |
| Ogus (2004) | Ogus, I. Anthony, *Regulation: Legal form and economic theory*, Hart 2004. [*Sitert etter: Gellert, Raphaël, The risk based* |

*approach to data protection, Oxford 2020 s. 89*]

Skullerud mfl. (2018) Skullerud, Åste Marie Bergseng, Cecilie Rønnevik, Jørgen Skorstad & Marius Eng Pellerud. *Personvernforordningen (GDPR): Kommentarutgave*, Universitetsforlaget 2018

Wessel-Aas & Ødegaard (2018) Wessel-Aas, Jon & Magnus Ødegaard. *Personvern; Publisering og behandling av personopplysninger*, 1. utgave, Gyldendal 2018

### 10.6.2 Artikler

Kuner (2008) Kuner, Christopher, *The 'internal morality' of European data protection law*, 24.11.2008 DOI: https://dx.doi.org/10.2139/ssrn.1443797

Robinson m. fl. (2009) Robinson, Neil, Hans Graux, Maarten Botterman, and Lorenzo Valeri, *Review of the European Data Protection Directive*, *RAND Corporation*, 2009 https://www.rand.org/pubs/technical_reports/TR710.html)

Bamberger og Mulligan (2013) Bamberger, Kenneth A. og, Deirdre K. Mulligan, «Privacy in Europe: Initial data on governance choices and corporate practices», *George Washington law review, vol. 81,* UC Berkeley public law

research paper no. 2328877, s. 1529-1664 https://ssrn.com/abstract=2328877)

Fredriksen (2013) — Fredriksen, Halvard Haukeland, «Betydningen av EUs pakt om grunnleggende rettigheter for EØS-retten», *Jussens Venner* 2013, s. 371-399 https://www.idunn.no/jv/2013/06/betydningen_av_eus_pakt_om_grunnleggende_rettigheter_for_eoe

European Union Agency for Fundamental Rights (2015) — European Union Agency for Fundamental Rights, *Freedom to conduct a business: exploring the dimensions of a fundamental right,* Luxemburg 2015 https://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-freedom-conduct-business_en.pdf

Gellert (2017) — Gellert, Raphaël, «Why the GDPR risk-based approach is about compliance risk, and why it´s not a bad thing», *Trends and Communities of legal informatics: IRIS 2017 – Proceedings of the 20th international legal informatics symposium,* 2017, s. 527-532 https://www.researchgate.net/publication/314839054_Why_the_GDPR_risk-based_approach_is_about_compliance_risk_and_why_it's_not_a_bad_thing

Quelle (2018) — Quelle, Claudia, «Enhancing compliance under the General Data Protection Regulation: The risky upshot of the

accountability- and risk-based approach», *European Journal of Risk Regulation, vol. 9, issue 3: Symposium on effective law and regulation,* Cambridge 2018, s. 502-526 DOI: https://doi.org/10.1017/err.2018.47

Gonçalves (2019) — Gonçalves, Maria Eduarda, «The risk-based approach under the new EU data protection regulation: a critical perspective», *Journal of risk research, vol. 23, issue 2, 2019*, s. 139-152. DOI: https://doi.org/10.1080/13669877.2018.1517381

Christakis (2020) — Christakis, Theodore, «*Schrems III»? First thoughts on the EDBP post-Schrems II recommendations on international data transfers – part 2,* 16.11.2020 https://europeanlawblog.eu/2020/11/16/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-2/ (sist lest 11.03.2021)

Tene (2020) — Omer Tene, *Quick reaction to EDPB Schrems II guidance* 12.11.2020 https://www.linkedin.com/pulse/quick-reaction-edpb-schrems-ii-guidance-omer-tene/?utm_source=POLITICO.EU&utm_campaign=a48677014b-EMAIL_CAMPAIGN_2020_11_13_02_43&utm_medium=email&utm_term=0_109

59edeb5-a48677014b-190373637) (sist lest 16.03.2021)

Foss (2021) — Foss, Kristian, «Fra konsesjon til Schrems II – eksport av personopplysninger i det 21. århundre», *Lov&Data 2021 nr. 1*, s. 17-25 https://lovdata.no/pro/#document/JUS/lod-2021-145-17?searchResultContext=77418780&rowNumber=1&totalHits=69 (sist lest 13.04.2021)

Hörnle (2021a) — Hörnle, Julia, *The jurisdictional challenge of internet regulation*, 24. mars 2021 https://blog.oup.com/2021/03/the-jurisdictional-challenge-of-internet-regulation/?fbclid=IwAR0IyU_UGLBzyur3bNKG166h7c6_B510dhRdgnuMe4Z3MW_6dSFElm8bXgI (sist lest 29.03.2021)

Rubinstein og Margulies (2021) — Rubinstein, Ira and Margulies, Peter, *Risk and rights in transatlantic data transfers: EU Privacy Law, U.S. surveillance, and the search for common ground*, 16.02.2021. Roger Williams Univ. Legal Studies Paper Forthcoming. DOI: https://dx.doi.org/10.2139/ssrn.3786415 (sist lest 12.03.2021)

### 10.6.3 Rapporter

CIPL (2014) — Centre for Information Policy Leadership (CIPL), *A risk-based approach to privacy: Improving effectiveness in practice*, 08.10.2014 (kan lastes ned her: https://www.ftc.gov/system/files/documents/public_comments/2014/10/00048-92775.pdf)

Digital Europe (2020) — Digital Europe, *Schrems II impact survey report*, 26.11.2020 (kan lastes ned her: https://www.digitaleurope.org/wp/wp-content/uploads/2020/11/DIGITALEUROPE_Schrems-II-Impact-Survey_November-2020.pdf)

U.S. Government (2020) — U.S. Department of Commerce, U.S. Department of Justice, Office of the Director of National Intelligence, *Information on U.S. privacy safeguards relevant to SCCs and other EU legal bases for EU-U.S. data transfers after Schrems II*, White Paper 2020 (kan lastes ned her: https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF)

CIPL (2020) — Centre for Information Policy Leadership, *A path forward for international data transfers under the GDPR after the CJEU Schrems II decision,* White Paper 2020 (kan lastes ned her:

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_gdpr_transfers_post_schrems_ii__24_september_2020__2_.pdf)

## 10.7 Øvrige kilder

Datatilsynet (2012) — Datatilsynet, *Kryptering.* 24.01.2012 https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/kryptering/ (sist lest 01.04.2021)

Regjeringen (2014) — Regjeringen, *EØS-samarbeidet,* 04.12.2014 https://www.regjeringen.no/no/tema/europapolitikk/eos1/eos-samarbeidet/id2339959/ (sist lest 12.02.2021)

Goodin (2015) — Goodin, Dan, *How the NSA can break trillions of encrypted web and VPN connections*, 15.10.2015 https://arstechnica.com/information-technology/2015/10/how-the-nsa-can-break-trillions-of-encrypted-web-and-vpn-connections/ (sist lest 15.03.2021)

Datatilsynet (2018) — Datatilsynet, *Skytjenester,* 23.06.2018 https://www.datatilsynet.no/personvern-pa-ulike-omrader/internett-og-apper/skytjenester/ (sist lest 22.04.2021)

Datatilsynet (2018a) — Datatilsynet, *Verktøy og metoder for godt personvern i kunstig intelligens,* 25.06.2018 https://www.datatilsynet.no/regelverk-og-verktoy/rapporter-og-utredninger/kunstig-intelligens/verktoy-og-metoder/ (sist lest 03.05.2021)

Regjeringen (2019) — Regjeringen, *Hva er personvern?* 30.10.2019 https://www.regjeringen.no/no/tema/statlig-forvaltning/personvern/hva-er-personvern/id448290/ (sist lest 20.04.2021)

Restad, Notaker og Mæhlum (2019) — Restad, Hilde, Hallvard Notaker, Lars Mæhlum: *Edward Snowden*, 30.01.2015 https://snl.no/Edward_Snowden (sist lest 02.04.2021)

Datatilsynet (2019) — Datatilsynet, *Det Europeiske Personvernrådet,* 03.05.2019 https://www.datatilsynet.no/regelverk-og-verktoy/internasjonalt/personvernradet/?fbclid=IwAR3gkrjA-GCYIQ65FCkQuIe51_nmok8ZLxrCXPQS3XzA4ObYTXVEnLajkFU (sist lest 15.02.2021)

Datatilsynet (2020) — Datatilsynet, *Spesielt om overføringer av opplysninger til utlandet* 27.07.2020 https://www.datatilsynet.no/rettigheter-og-

plikter/virksomhetenes-plikter/overfore/ (sist lest 02.02.2021)

Datatilsynet (2020a) — Datatilsynet, *Spørsmål og svar om nye regler for overføring av personopplysninger til land utenfor EU/EØS,* 22.10.2020 https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/sos-om-nye-regler-for-overforing/ (sist lest 22.04.2021)

Nasjonal Sikkerhetsmyndighet (2020) — Nasjonal Sikkerhetsmyndighet, *Helhetlig digitalt risikobilde 2020.* https://nsm.no/regelverk-og-hjelp/rapporter/helhetlig-digitalt-risikobilde-2020/skytjenester-og-tjenesteutsetting-muligheter-og-utfordringer/ (sist lest 01.05.2021)

Meld. St. 22 (2020-2021) — Melding til Stortinget (2020-2021), *Data som ressurs – Datadrevet økonomi og innovasjon*, 26.02.2021. https://www.regjeringen.no/no/dokumenter/meld.-st.-22-20202021/id2841118/